MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDANTE DO EXÉRCITO

INSTRUÇÕES GERAIS PARA A SALVAGUARDA DE ASSUNTOS SIGILOSOS

2ª Edição
2023

EB10-IG-01.011

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COMANDANTE DO EXÉRCITO

INSTRUÇÕES GERAIS PARA A SALVAGUARDA DE ASSUNTOS SIGILOSOS

2ª Edição
2023

(Publicado no Boletim do Exército nº 52, de 29 de dezembro de 2023)

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COMANDANTE DO EXÉRCITO

PORTARIA – C Ex Nº 2.145, DE 18 DE DEZEMBRO DE 2023

EB: 64535.041974/2022-10

Aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), 2ª edição, 2023.

O COMANDANTE DO EXÉRCITO, no uso das atribuições que lhe conferem o art. 4º da Lei Complementar nº 97, de 9 de junho de 1999, o art. 20, incisos I e XIV, do Anexo I, do Decreto nº 5.751, de 12 de abril de 2006, e considerando o que consta nos autos EB: 64535.041974/2022-10, resolve:

Art. 1º Aprovar as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), 2ª edição, 2023.

Art. 2º Revogar a Portaria – C Ex nº nº 1.067, de 8 de setembro de 2014.

Art. 3º Esta Portaria entra em vigor em 2 de janeiro de 2024.

Gen Ex TOMÁS MIGUEL MINÉ RIBEIRO PAIVA
Comandante do Exército

TOMAS MIGUEL MINE RIBEIRO PAIVA:56928963700
Eu estou aprovando este documento
2023.12.19 11:06:05-03'00'

FOLHA REGISTRO DE MODIFICAÇÕES (FRM)

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS A'1FETADAS	DATA

ÍNDICE DE ASSUNTOS

	Art.
CAPÍTULO I – DAS DISPOSIÇÕES GERAIS	
Seção I – Da Finalidade	1º
Seção II – Da Conceituação	2º
Seção III – Das Restrições de Acesso	3º
CAPÍTULO II – DAS INFORMAÇÕES CLASSIFICADAS	
Seção I – Das Condicionantes para a Classificação da Informação	4º/8º
Seção II – Da Competência para a Classificação da Informação	9º/10
Seção III – Dos Procedimentos para Classificação, Reclassificação, Desclassificação e Prorrogação do Prazo de Sigilo da Informação	
Subseção I – Da Classificação da Informação	11/20
Subseção II – Da Desclassificação e da Reavaliação da Informação Classificada	21/25
CAPÍTULO III – DAS DEMAIS SITUAÇÕES COM RESTRIÇÃO DE ACESSO	
Seção I – Das Informações Pessoais	26/30
Seção II – Das Informações Referentes a Projetos de Pesquisa e Desenvolvimento Científico ou Tecnológico	31/33
Seção III – Das Informações Contidas em Documentos Preparatórios	34/38
Seção IV – Das Áreas e Instalações de Acesso Restrito	39/40
Seção V – Dos Materiais de Acesso Restrito	41/42
CAPÍTULO IV – DAS MEDIDAS DE CONTROLE	
Seção I – Das Orientações Gerais	43/47
Seção II – Do Acesso	48/52
Seção III – Dos Documentos e Materiais Controlados	53/67
Seção IV – Das Marcações de Sigilo	68/73
CAPÍTULO V – DA SEGURANÇA DA INFORMAÇÃO	
Seção I – Da Segurança do Pessoal	
Subseção I – Da Segurança no Processo Seletivo	74/76
Subseção II – Da Segurança no Desempenho da Função	77/78
Subseção III – Da Segurança no Desligamento da Função	79
Seção II – Da Segurança da Documentação	
Subseção I – Das Medidas Gerais de Segurança da Documentação	80/81
Subseção II – Da Segurança na Produção	82/87
Subseção III – Da Segurança na Expedição e Recepção	88/97
Subseção IV – Da Segurança no Manuseio	98/105
Subseção V – Da Segurança no Arquivamento	106/107
Subseção VI – Da Segurança na Eliminação	108/113
Seção III – Da Segurança do Material	
Subseção I – Das Medidas Gerais de Segurança do Material	114/121

Subseção II – Da Segurança no Transporte..... 122/124
Subseção III – Da Segurança na Eliminação de Material Controlado..... 125
Seção IV – Da Segurança das Áreas e Instalações..... 126/128
Seção V – Da Segurança das Comunicações
Subseção I – Das Medidas Gerais de Segurança das Comunicações..... 129
Subseção II – Da Segurança na Remessa ou Transmissão..... 130/134
Subseção III – Da Segurança do Conteúdo..... 135/137
Seção VI – Da Segurança da Tecnologia da Informação e Comunicações
Subseção I – Da Segurança do Equipamento..... 138
Subseção II – Da Segurança do Software..... 139/140
Subseção III – Da Segurança Física..... 141/143
Subseção IV – Da Segurança na Rede Mundial de Computadores..... 144/145
Subseção V – Da Segurança no Correio Eletrônico, da Mensageria Eletrônica e do Armazenamento de Arquivo em Nuvem..... 146/150
Subseção VI – Da Segurança em Sistemas Corporativos, Intranet e Redes Sociais..... 151/158
Subseção VII – Da Segurança contra Furto, Roubo ou Extravio de Dados..... 159/162
Seção VII – Das Prescrições Diversas..... 163
CAPÍTULO VI – DA CELEBRAÇÃO DE CONTRATOS..... 164/168
CAPÍTULO VII – DAS DISPOSIÇÕES FINAIS..... 169/174

ANEXOS:

A – TERMO DE INVENTÁRIO DE DOCUMENTOS E/OU MATERIAIS CONTROLADOS
B – TERMO DE TRANSFERÊNCIA DE GUARDA DE DOCUMENTOS E/OU MATERIAIS CONTROLADOS
C – MARCAÇÃO PARA INFORMAÇÕES, MATERIAIS E ÁREAS SIGILOSAS
D – TERMO DE ELIMINAÇÃO DE CÓPIA(S) DE DOCUMENTO CONTROLADO
E – TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO
F – TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO
G – IDENTIFICAÇÃO DE CÓPIA DE DOCUMENTO SIGILOSO
H – TERMO DE ELIMINAÇÃO DE MATERIAL CONTROLADO
I – RESUMO EXPLICATIVO PARA PROPOSTA DE TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO
J – TERMO DE CUSTÓDIA DE MATERIAL/DOCUMENTO CONTROLADO

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Seção I
Da Finalidade

Art. 1º As presentes Instruções Gerais (IG) têm por finalidade regular o tratamento e o acesso às informações sigilosas.

Parágrafo único. Consideram-se sigilosas as informações classificadas, as enquadradas em hipóteses legais de sigilo (informação pessoal, de pesquisa e desenvolvimento, sigilo bancário, sigilo fiscal, segredo industrial, segredo de justiça, documento preparatório, entre outras), assim como as relacionadas à atividade de ~~i~~nteligência.

Seção II
Da Conceituação

Art. 2º Para a aplicação destas IG, adotam-se as seguintes conceituações:

I – **acesso** é a possibilidade ou oportunidade de obtenção de informação (conhecimento ou dado) sigilosa. Também é entendida como a possibilidade de usar os ativos de informação que contêm informação (conhecimento ou dado) sigilosa. Deriva, necessariamente, de uma autorização oficial emitida por uma autoridade competente ou da superação de medidas de salvaguarda. O termo denota a possibilidade, a oportunidade e a condição para que sejam obtidos ou consultados conhecimentos, dados ou materiais que devam estar protegidos;

II – **algoritmo criptográfico** é a função matemática utilizada na cifração e na decifração de informações sigilosas;

III – **algoritmo de Estado** é aquele desenvolvido pelo Estado, não comercializável e para uso exclusivo em interesse do serviço de órgãos ou entidades da administração pública federal , direta e indireta;

IV – **área ou instalação de acesso restrito** é aquela que, por conter documento ou material sigiloso, ou que, por sua utilização ou finalidade, demande proteção ao ato de ingressar, transitar, conhecer ou consultar a informação;

V – **área sigilosa** é a área na qual os dados, informações ou conhecimentos sigilosos contidos em documentos, materiais, ativos de informação e sistemas são tratados, manuseados, transmitidos ou guardados, uma vez que requerem medidas especiais de proteção e permissão de acesso;

VI – **assunto sigiloso** é aquele que, por sua natureza, deve ser de conhecimento restrito e, portanto, requer adoção de medidas especiais de salvaguarda;

VII – **ativos de informação** são os meios de armazenamento, transmissão e processamento de dados e informação, os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão), os sistemas utilizados para tal, os sistemas de informação seguros, bem como os locais nos quais se encontram esses meios e as pessoas que a eles têm acesso;

VIII – **cifra** é o sistema criptográfico no qual as letras de cada palavra de um texto em claro são substituídas por outras letras, símbolos ou algarismos, segundo regra ou convenção predeterminada, para se obter um texto criptografado;

IX – **cifração** é o ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir linguagem em claro por outra, ininteligível para pessoas não

autorizadas a conhecê-la;

X – **classificação** é o ato deatribuir grau de sigilo à informação que requeira medidas especiais de salvaguarda e, por consequência, ao documento, material ou área que a contenha, utilize ou veicule;

XI – **código de indexação** é o código alfanumérico que indexa documento com informação classificada, em qualquer grau de sigilo;

XII – **comprometimento** é a perda de segurança, resultante do acesso não autorizado;

XIII – **contrato sigiloso** é o ajuste, convênio ou termo de cooperação, cujo objeto ou execução implique tratamento de informação sigilosa;

XIV – **credencial de segurança** é o certificado que autoriza uma pessoa a acessar e realizar o tratamento de informação classificada, de acordo com o nível de necessidade;

XV – **credenciamento de segurança** é o processo utilizado para habilitar órgão ou entidade, públicos ou privados, e credenciar pessoa para o tratamento de informação classificada;

XVI – **custódia** é a responsabilidade pela guarda de documento ou de material sigiloso;

XVII – **dado pessoal** é a informação relacionada à pessoa natural, identificada ou identificável;

XVIII – **dado pessoal sensível** é aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, saúde ou vida sexual, genética ou biometria, quando vinculado a uma pessoa natural;

XIX – **decifração** é o ato de decifrar, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, revertendo processo de cifração original;

XX – **desclassificação** é o ato pelo qual a autoridade, responsável pela classificação de uma informação, retira-lhe o grau de sigilo atribuído anteriormente, tornando-a ostensiva ou de acesso restrito;

XXI – **detentor** é a pessoa responsável pela custódia de documento ou material;

XXII – **detentor direto** é a pessoa encarregada da custódia física de um documento ou material;

XXIII – **detentor indireto** é a pessoa que, ao receber um documento ou material, transfere, por necessidade do serviço, sua custódia para um detentor direto;

XXIV – **dispositivo móvel** é o equipamento portátil dotado de capacidade computacional ou dispositivo removível de memória para armazenamento, entre os quais se incluem, não limitando a estes: **notebooks**, **netbooks**, **smartphones**, **tablets**, **pen drives**, **USB drives**, **hard disk** (HD) externo, memórias SSD e cartões de memória;

XXV – **documento** é a unidade de registro de informação, em qualquer suporte material ou formato, podendo ser textual, cartográfico, iconográfico, filmográfico, cinematográfico, audiovisual, fotográfico, imagem, sonoro, micrográfico, digital ou eletrônico;

XXVI – **documento controlado (DC)** é todo e qualquer documento sigiloso que, por sua importância, necessita de medidas adicionais de controle;

XXVII – **documento de Inteligência** é aquele utilizado para veicular informação de Inteligência;

XXVIII – **documento preparatório** é o documento formal, utilizado como fundamento para a tomada de decisão ou de ato administrativo;

XXIX – **documento sigiloso** é aquele que requer medidas adicionais de controle, devendo ser de acesso restrito ou receber classificação;

XXX – **eliminação** é o ato de se destruir documento que foi considerado sem valor para fins de arquivo e/ou consulta, ou material que não mais atenda à finalidade a que se destina;

XXXI – **gestão documental** é o conjunto de procedimentos e operações técnicas referentes à produção, tramitação, classificação, acesso, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando à sua eliminação ou recolhimento para guarda permanente;

XXXII – **grau de sigilo** é a gradação atribuída a dados, conhecimentos, materiais, áreas ou instalações, considerados sigilosos, em decorrência de sua natureza ou conteúdo;

XXXIII – **informação** é o dado, processado ou não, que pode ser utilizado para produção e transmissão de conhecimento, contido em qualquer meio, suporte ou formato;

XXXIV – **informação classificada** é aquela sigilosa em poder do órgão ou entidade pública, que recebeu de autoridade competente a classificação no grau de sigilo ultrassecreto, secreto ou reservado, devido ao seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado;

XXXV – **informação de acesso restrito** é aquela que, não sendo passível de receber classificação sigilosa, encontra-se abrangida por hipótese legal de sigilo;

XXXVI – **informação de caráter funcional** é aquela relacionada ao militar e ao servidor, derivada do exercício da sua atividade estatal, vinculada a ato de serviço ou decorrente de situação funcional;

XXXVII – **informação pessoal** é aquela relacionada à pessoa natural identificada ou identificável;

XXXVIII – **informação sigilosa** é aquela submetida, temporariamente, à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade ou do Estado, ou por ser abrangida pelas demais hipóteses legais de sigilo;

XXXIX – **investigação para credenciamento de segurança** é o procedimento de averiguação da existência de requisitos indispensáveis para a concessão da credencial de segurança à pessoal natural, para o acesso e o tratamento de informação classificada;

XL – **material controlado (MC)** é todo material sigiloso que, por sua importância, necessita de medidas adicionais de controle;

XLI – **material de acesso restrito** é aquele que, não sendo passível de receber classificação sigilosa, demanda medidas especiais de proteção, por sua utilização ou finalidade;

XLII – **marcação** é a aposição de marca que indica o grau de sigilo da informação classificada, ou o amparo legal que permite a imposição de restrição de acesso ao seu conteúdo;

XLIII – **medida de segurança** é a ação destinada a garantir o sigilo, a inviolabilidade, a integridade, a autenticidade e a disponibilidade da informação sigilosa;

XLIV – **necessidade de conhecer** é a condição pessoal, inerente ao efetivo exercício de cargo, da função, do emprego ou da atividade, indispensável para que uma pessoa tenha acesso à informação sigilosa;

XLV – **órgão controlador** é a organização militar (OM) que elabora e expede um DC ou a responsável pelo controle de um MC;

XLVI –**quebra de segurança** é a ação ou omissão que implica no comprometimento, ou no risco de comprometimento, de informação sigilosa;

XLVII – **reclassificação** é o ato pelo qual a autoridade competente altera a classificação original de uma informação, podendo atribuir grau de sigilo superior ou inferior;

XLVIII – **recurso criptográfico** é o sistema, programa, processo e/ou equipamento, isolado ou em rede, que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XLIX – **restrição de acesso** é o ato de limitar ou impedir o contato de uma pessoa não credenciada ou não autorizada com documento, área, instalação ou material, segundo as normas legais vigentes;

L – **tratamento de dados pessoais** é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

LI – **tratamento da informação classificada** é o conjunto de ações referentes à produção, recepção, classificação, desclassificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada;

LII – **segurança da informação e das comunicações** é o conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, inviolabilidade, integridade, confiabilidade e autenticidade das informações;

LIII – **sigilo** é a inviolabilidade do conhecimento ou dado contido nos documentos, assegurada por lei; do conhecimento restrito a pessoas credenciadas; e da proteção contra revelação não autorizada; e

LIV – **visitante** é a pessoa cuja entrada foi admitida, em caráter excepcional e sob condições específicas, em área sob restrição de acesso.

Seção III
Das Restrições de Acesso

Art. 3º O Exército Brasileiro (EB) manterá sob restrição de acesso, independentemente de classificação, os ativos de informação, o documento, o material, a área ou a instalação sob sua custódia, que contenha:

I – informação classificada;

II – informação pessoal ou dado pessoal;

III – informação protegida por legislação específica como de natureza sigilosa, tal como sigilo bancário, fiscal ou patrimonial etc;

IV – processo judicial sob segredo de justiça;

V – identificação do denunciante que origine procedimento investigativo;

VI – papel de trabalho e procedimento relativo a ações de controle e de inspeção correcional, ou de qualquer espécie de ação investigativa, nos termos do art. 26, § 3º, da Lei nº 10.180, de 6 de fevereiro de 2001;

VII – relatório e nota técnica decorrente de investigação, auditoria, fiscalização e outros documentos, relativos à atividade de correição;

VIII – informação ou acesso a instalações referentes a projeto de pesquisa e desenvolvimento científico ou tecnológico, de interesse da defesa nacional;

IX – documento preparatório;

X – documento ou informação de natureza técnica, produzido por órgão ou entidade não vinculado, ainda que não se caracterize a custódia;

XI – documento de inteligência;

XII – área e instalação que contenha informação sigilosa;

XIII – informação constante de manual de instrução ou de documento que trate do emprego de material de acesso restrito;

XIV – materiais sigilosos;

XV – ativos de informação classificado; e

XVI – correspondência pessoal e outras, abrangidas pelas demais hipóteses legais de sigilo.

Parágrafo único. Cabe às autoridades mencionadas nos art. 9º e 10 destas IG definir a adoção de medidas de restrição de acesso, dentro dos preceitos estabelecidos nos dispositivos legais vigentes.

CAPÍTULO II
DAS INFORMAÇÕES CLASSIFICADAS

Seção I
Das Condicionantes para a Classificação da Informação

Art. 4º Os graus de sigilo para a classificação de informação são:

I – RESERVADO;

II – SECRETO; e

III – ULTRASSECRETO.

Art. 5º Somente será passível de classificação a informação considerada imprescindível à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possa:

I – pôr em risco a defesa, a soberania ou a integridade do território nacional;

II – prejudicar ou pôr em risco a condução de negociação ou as relações internacionais do País, ou a informação que tenha sido fornecida, em caráter sigiloso, por outro Estado e organismo internacional;

III – pôr em risco a vida, a segurança ou a saúde da população;

IV – oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

V – prejudicar ou causar risco a plano ou operação estratégica das Forças Armadas;

VI – prejudicar ou causar risco a projeto de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistema, bem, instalação ou área de interesse estratégico nacional;

VII – pôr em risco a segurança de instituição, de alta autoridade nacional ou estrangeira e seus familiares; ou

VIII – comprometer atividade de inteligência, de investigação ou fiscalização em andamento relacionada com a prevenção ou repressão de infrações.

Art. 6º Para a classificação da informação deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:

I – a gravidade do risco ou dano à segurança da sociedade ou do Estado; e

II – o prazo máximo de restrição de acesso ou o evento que defina seu termo final.

Art. 7º Quanto à gravidade do risco, ou dano à segurança da sociedade ou do Estado:

I – será classificada no grau de sigilo ULTRASSECRETO a informação, material, ativo de informação ou instalação cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave a(à)(s):

a) soberania e integridade territorial nacionais;

b) relações internacionais do País;

c) plano e operação militar que afetem as alíneas “a” e “b” do presente inciso;

d) projeto de pesquisa, instalação ou desenvolvimento científico e tecnológico de interesse da defesa nacional; e

e) programa econômico;

II – será classificada no grau de sigilo SECRETO a informação cujo conhecimento não autorizado possa acarretar dano grave a:

a) sistema;

b) instalação;

c) programa;

d) projeto;

e) plano ou operação de interesse da defesa nacional;

f) assunto diplomático e de inteligência; e

g) plano ou seus detalhes;

III – será classificada no grau de sigilo RESERVADO a informação cujo conhecimento não autorizado possa acarretar dano, tal como a que frustre ou comprometa:

a) objetivo de interesse do Poder Executivo;

b) objetivo ou atividade de interesse do Comando do Exército; e

c) plano, operação ou objetivo nele previsto ou referido.

Art. 8º Os prazos máximos de restrição de acesso à informação classificada vigoram na data de sua produção e são os seguintes:

I – para o grau de sigilo ULTRASSECRETO: 25 (vinte e cinco) anos;

II – para o grau de sigilo SECRETO: 15 (quinze) anos; e

III – para o grau de sigilo RESERVADO: 5 (cinco) anos.

§ 1º Somente a informação classificada no grau de sigilo ULTRASSECRETO é passível de ter o seu prazo prorrogado, por uma única vez.

§ 2º A informação que puder colocar em risco a segurança do Presidente e do Vice-Presidente da República, seus respectivos cônjuges e filhos será classificada no grau de sigilo RESERVADO e ficará sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.

§ 3º Poderá ser estabelecida como termo final de restrição de acesso à ocorrência de determinado evento, observados os prazos máximos de classificação.

§ 4º Transcorrido o prazo máximo de classificação, a informação tornar-se-á automaticamente de acesso público, dentro das prescrições da legislação vigente, observadas as restrições de acesso previstas no art. 3º destas IG.

Seção II
Da Competência para a Classificação da Informação

Art. 9º O Comandante do Exército tem competência para classificar a informação sigilosa nos graus de sigilo ULTRASSECRETO, SECRETO e RESERVADO, sendo vedada a delegação de competência para a classificação nos graus de sigilo ULTRASSECRETO e SECRETO.

Art. 10. O comandante (Cmt), chefe (Ch), diretor (Dir) de OM ou oficial-general tem competência para classificar informação sigilosa no grau RESERVADO, sendo vedada a delegação ou a assinatura no impedimento do documento classificado e do Termo de Classificação de Informação (TCI).

§ 1º A autoridade que responde pelo comando, quando essa situação estiver publicada em boletim interno (BI) da OM, poderá classificar informação sigilosa.

§ 2º O oficial-general, Cmt, Ch ou Dir de OM deverá dar ciência do seu ato de classificação de documento no grau RESERVADO ao Comandante do Exército, no prazo de 90 (noventa) dias, por intermédio do Centro de Inteligência do Exército (CIE), fazendo sua implantação no sistema de controle de documentos classificados do Exército.

§ 3º A classificação de informação no grau de sigilo ULTRASSECRETO, pelo Comandante do Exército, deverá ser ratificada pelo Ministro da Defesa no prazo de 30 (trinta) dias.

§ 4º Enquanto não ratificada, a classificação de que trata o § 3º deste artigo considera-se válida para todos os efeitos legais.

Seção III
Dos Procedimentos para Classificação, Reclassificação, Desclassificação e Prorrogação do Prazo de Sigilo da Informação

Subseção I
Da Classificação da Informação

Art. 11. A decisão de classificar a informação deverá ser formalizada pela emissão de TCI, que conterá os seguintes itens:

I – código de indexação de documento;

II – grau de sigilo;

III – categoria na qual se enquadra a informação;

IV – tipo de documento;

V – data da produção;

VI – indicação de dispositivo legal que fundamenta a classificação;

VII – razão da classificação, observados os critérios estabelecidos no art. 6º, com a justificativa para o grau de sigilo adotado;

VIII – assunto a que se refere a informação, com a descrição de elementos mínimos que permitam a identificação do tema de que trata a classificação;

IX – indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, observados os limites previstos no art. 8º;

X – data da classificação; e

XI – identificação da autoridade que classificou a informação.

§ 1º A informação prevista no inciso VII do **caput** deverá ser mantida no mesmo grau de sigilo da informação classificada.

§ 2º A informação somente será considerada classificada após a assinatura do respectivo TCI.

§ 3º O TCI é único para cada documento classificado.

§ 4º Para confecção do TCI, a informação a ser classificada deverá receber número único de protocolo (NUP)/número único de documento (NUD), mesmo que não seja um documento padrão, como esboço, desenho, mapa, carta, fotografia, imagem, negativo ou **slide.**

§ 5º A competência para a assinatura do TCI é das autoridades previstas nos art. 9º e 10 destas IG.

§ 6º O TCI deverá ser confeccionado em 3 (três) vias, conforme modelo contido no Anexo F destas IG.

Art. 12. O documento RESERVADO terá a 1ª via do TCI arquivada na OM que o produziu, a fim de possibilitar sua atualização e controle (reclassificação, desclassificação ou redução do prazo).

Parágrafo único. A 2ª via do TCI seguirá anexada à informação e a 3ª via deve ser remetida à Comissão Permanente de Avaliação de Documentos Classificados do Exército (CPADC) do CIE.

Art. 13. Para a classificação da informação nos graus de sigilo SECRETO e ULTRASSECRETO, deverão ser seguidos os seguintes procedimentos:

I – o Comandante Militar de Área, Ch ou Dir de Órgão de Direção Geral (ODG), Órgão de Direção Operacional, órgão de direção setorial (ODS) ou órgão de assistência direta e imediata ao Comandante do Exército deverá analisar a proposta de classificação nos graus de sigilo SECRETO e ULTRASSECRETO de suas OM subordinadas;

II – confirmada a necessidade de classificação nesses graus de sigilo, enviar proposta de TCI, pela rede segura do Exército, à CPADC/CIE;

III – a CPADC/CIE imprimirá o TCI e o encaminhará, acompanhado do "resumo explicativo", ao Gabinete do Comandante do Exército (Gab Cmt Ex) para a assinatura pelo Comandante; e

IV – o Gab Cmt Ex devolverá o TCI assinado à CPADC/CIE, que adotará os seguintes procedimentos:

a) para a informação no grau de sigilo ULTRASSECRETO, encaminhará o TCI ao Ministro da Defesa para ratificação no prazo de 30 (trinta) dias, contados a partir da data de classificação;

b) para a informação no grau de sigilo SECRETO, encaminhará cópia do TCI à Comissão Mista de Reavaliação de Informações (CMRI), instituída nos termos do art. 32 do Decreto nº 7.724, de 16 de maio de 2012, no prazo de 30 (trinta) dias, contados da data de classificação;

c) enviará cópia assinada do TCI ao comando correspondente e à Controladoria-Geral da União (CGU); e

d) arquivará o TCI original.

Art. 14. Na confecção do TCI para a informação no grau de sigilo SECRETO ou ULTRASSECRETO, deverão ser observados os seguintes aspectos:

I – na proposta, os campos “RAZÕES PARA A CLASSIFICAÇÃO” e “DATA DE CLASSIFICAÇÃO” devem estar em branco;

II – a proposta deve ser acompanhada de “resumo explicativo”;

III – o “resumo explicativo” deve seguir o modelo do Anexo I; contendo:

a) o assunto de que trata o documento;

b) a proposta de razão para a classificação; e

c) os riscos observados e a visualização dos possíveis danos à segurança da sociedade ou do Estado;

IV – o “resumo explicativo” consubstanciará as razões para se classificar o documento, devendo ser preciso e conciso.

Art. 15. A informação classificada receberá o Código de Indexação de Documento que Contém Informação Classificada (CIDIC), conforme modelo constante do Anexo F.

Art. 16. O CIDIC será composto por elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada e será estruturado em 2 (duas) partes:

I – a primeira parte será composta pelo NUP, originalmente cadastrado conforme legislação de gestão documental; e

II – a segunda parte será composta dos seguintes elementos:

a) grau de sigilo: indicação do grau de sigilo, ULTRASSECRETO, SECRETO ou RESERVADO, grafados em vermelho;

b) categoria: indicação, com 2 (dois) dígitos, da categoria relativa ao primeiro nível do Vocabulário Controlado do Governo Eletrônico, conforme o Anexo II do Decreto nº 7.845, de 14 de novembro de 2012;

c) data de produção: registrar no formato dia (dois dígitos) / mês (dois dígitos) / ano (quatro dígitos);

d) data de desclassificação: registrar a potencial data de desclassificação do documento, no formato dia (dois dígitos) / mês (dois dígitos) / ano (quatro dígitos);

e) indicação de reclassificação (visualização de futura necessidade de reclassificação):

1) reclassificação de documento resultante de reavaliação; ou

2) primeiro registro da classificação;

f) indicação da data de prorrogação da manutenção da classificação: indicação, exclusivamente para informação classificada no grau de sigilo ultrassecreto, no formato dia (dois dígitos) / mês (dois dígitos) / ano (quatro dígitos), na cor vermelha, quando possível.

§ 1º O documento classificado, quando de sua desclassificação, manterá apenas o NUP.

§ 2º Não será utilizada tabela de classificação de assunto ou de natureza do documento, em razão de exigência de restrição temporária de acesso a documento classificado, sob pena de pôr em risco sua proteção.

§ 3º No que concerne à gestão documental, deverá ser guardado o histórico de alterações do CIDIC.

Art. 17. As autoridades previstas nos art. 9º e 10 destas IG, ao classificar a informação, deverão enviar, imediatamente, as informações previstas no **caput** do art. 11 para a CPADC/CIE.

Art. 18. A CPADC/CIE, após receber o TCI das informações classificadas em qualquer grau de sigilo, deverá enviar, no prazo de 30 (trinta) dias, contado da data da decisão de classificação ou de sua ratificação, as informações previstas no **caput** do art. 11 à:

I – CMRI, no caso de informações classificadas no grau ultrassecreto ou secreto; ou

II – CGU, no caso de informações classificadas em qualquer grau de sigilo, ressalvado o envio das informações de que trata o inciso VII do **caput** do art. 11 destas IG.

§ 1º Na hipótese de que trata o inciso II do caput deste artigo, a CPADC/CIE, quando identificar, a partir do exame dos elementos públicos que compõem o TCI, indícios de erro na classificação da informação, deverá notificar a autoridade classificadora, que decidirá sobre a reavaliação da classificação, no prazo de 10 (dez) dias.

§ 2º Os indícios de erro a que se refere o § 1º serão considerados quanto:

I – ao não enquadramento do assunto de que trata o inciso VIII do **caput** do art. 11 nas hipóteses legais de sigilo; e

II – a não adequação do grau de sigilo.

Art. 19. O disposto no inciso VII-A do **caput** do art. 31 do Decreto nº 7.724, de 2012, não incidirá sobre o(s) TCI produzidos antes da data de publicação do Decreto nº 11.527, de 16 de maio de 2023.

Art. 20. O disposto na alínea "e" do inciso II do **caput** do art. 45 do Decreto nº 7.724, de 2012, (assunto da informação classificada) não incidirá sobre os róis de informações classificadas publicados em sítio eletrônico antes da data de entrada em vigor do referido dispositivo.

Subseção II
Da Desclassificação e da Reavaliação da Informação Classificada

Art. 21. A classificação da informação será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou ofício, para desclassificação ou redução do prazo de sigilo.

Parágrafo único. Para o cumprimento do disposto no **caput**, além do previsto no art. 6º, deverá ser observado:

I – o prazo máximo de restrição de acesso à informação, previsto no art. 8º;

II – o prazo máximo de 4 (quatro) anos para revisão de ofício da informação classificada no grau de sigilo ULTRASSECRETO ou SECRETO, previsto no inciso I do **caput** do art. 47 do Decreto nº 7.724, de 2012;

III – a permanência das razões da classificação;

IV – a possibilidade de danos ou riscos decorrentes da divulgação ou acesso irrestrito da informação; e

V – a peculiaridade da informação produzida no exterior por autoridade ou agente público.

Art. 22. Os procedimentos para reavaliação e desclassificação de informação classificada serão os previstos na legislação específica de avaliação e controle de documentos classificados do Exército.

Art. 23. O pedido de desclassificação ou de reavaliação da classificação de informação poderá ser apresentado ao órgão ou entidade, independentemente de existir prévio pedido de acesso à

informação.

§ 1º O pedido de que trata o **caput** será endereçado à autoridade classificadora, que deverá tomar sua decisão no prazo de 30 (trinta) dias.

§ 2º No caso de informação produzida por autoridade ou agente público no exterior, o requerimento de desclassificação e reavaliação será apreciado pela autoridade hierarquicamente superior que estiver em território brasileiro.

Art. 24. Negado o pedido de desclassificação ou de reavaliação da informação pela autoridade classificadora, o requerente poderá apresentar recurso no prazo de 10 (dez) dias, contado da ciência da negativa, primeiramente perante o Comandante do Exército e, em caso de negativa, ao Ministro de Estado da Defesa.

§ 1º Será apresentada uma decisão no prazo de 30 (trinta) dias, após a apreciação do recurso.

§ 2º Desprovido o recurso de que trata o **caput**, poderá o requerente apresentar recurso à CMRI, no prazo de 10 (dez) dias, contado da ciência da decisão.

Art. 25. A decisão sobre a desclassificação, a reclassificação ou a redução do prazo de sigilo de informação classificada deverá constar da capa do processo, se houver, e do campo apropriado no TCI.

CAPÍTULO III
DAS DEMAIS SITUAÇÕES COM RESTRIÇÃO DE ACESSO

Seção I
Das Informações Pessoais

Art. 26. O tratamento da informação pessoal deve assegurar a sua proteção, observadas a disponibilidade, a autenticidade, a integridade e as restrições de acesso.

§ 1º A informação pessoal de militar e de servidor, que não decorrer do exercício de sua função, terá seu acesso restrito, independente de classificação de sigilo, pelo prazo máximo de 100 (cem) anos, a contar da data de sua produção.

§ 2º Terão acesso à informação pessoal os militares ou servidores que, devidamente autorizados, têm a necessidade de conhecer seu conteúdo por força de atribuição funcional. Também terá acesso a pessoa a quem essa informação se refere, observando-se as disposições da Lei nº 13.709, de 14 de agosto de 2018, os termos do art. 31 da Lei nº 12.527, de 18 de novembro de 2011, e dos art. 55 a 62 do Decreto nº 7.724, de 2012.

§ 3º Serão observadas as ações previstas na Diretriz de Orientação para Aplicação da Lei Geral de Proteção de Dados Pessoais no Exército Brasileiro (EB20-D-02.013), aprovada pela Portaria - EME nº 88, de 7 de maio de 2020, decorrentes da Lei nº 13.709, de 2018, visando proteger as informações pessoais de integrantes do EB e de usuários de serviços do EB que, por força normativa, forneçam informações pessoais aos órgãos internos da Força e as informações pessoais oriundas de compartilhamento de dados entre órgãos e entidades da administração pública.

Art. 27. O documento que contenha informação pessoal deverá receber marcação nas partes superior e inferior de todas as páginas, existindo ou não classificação de sigilo, conforme modelo do Anexo C.

Art. 28. A informação de militar ou servidor, de caráter funcional, é considerada de interesse público, constituindo-se documentação governamental e bem público de natureza imaterial.

Art. 29. A informação de caráter funcional será publicada em BI da OM, quando

relacionada a:

I – dado da carreira do militar e servidor relacionado ao exercício de sua atividade na administração pública;

II – todo registro de informação referente à dinâmica da carreira do militar e da carreira do servidor civil vinculado ao EB, como medalhas, Teste de Avaliação Física, Teste de Aptidão de Tiro, elogio, trabalho útil, próprio nacional residencial (sem citar o endereço), licença-adotante, licença-paternidade, licença-gestante, férias, quadro, armas, serviços, especialidades e categorias de oficiais/ qualificação militar para subtenentes e sargentos, convalescença e baixa ao hospital (sem citar a doença), dispensa como recompensa, desconto em férias, núpcias, luto, instalação, dispensa do serviço em decorrência de prescrição médica (sem citar a doença), exercício da função, horas de voo, horas de raios X, horas de mergulho, salto com paraquedas, índice de proficiência linguística, promoção, dilação de estágio atual, licenciamento, desligamento, apresentação por término de trânsito, situações regulamentares, missão no exterior, movimentação, tempo de serviço público anterior à convocação do estágio atual, convocação do estágio atual, prorrogação do estágio atual, apresentação anual e outros que não se refiram à intimidade, à vida pessoal, à honra e à imagem; e

III – outras informações relacionadas a ato praticado pela administração que devam ser publicadas, observado o disposto no inciso XXXIV do art. 2º destas IG.

Art. 30. Será publicada em boletim de acesso restrito (BAR) da OM a informação pessoal, de militar ou servidor, pertinente a:

I – código pessoal, número do CPF, foto, local de nascimento, filiação, tipo sanguíneo e fator RH, estado civil, escolaridade, título de eleitor, PIS-PASEP, religião, e-mail, telefone, endereço, dado bancário, documentação nosológica, data de vinculação à Seção de Inativos e Pensionistas /órgão pagador, OM de vinculação, informação sobre cônjuge e dependente, inclusão e exclusão de beneficiário, pensão alimentícia, dados relacionados à inspeção de saúde e reforma por motivo de saúde; e

II – outros dados não relacionados no inciso anterior, caso se enquadrem nas hipóteses legais de sigilo.

§ 1º Compete ao Cmt, Ch ou Dir de OM, assessorado pelo encarregado do pessoal e pelo oficial de inteligência da OM, analisar a informação não relacionada nos incisos anteriores, para decidir o devido tratamento e a correspondente publicação em BAR ou BI.

§ 2º Havendo necessidade de se publicar assunto classificado como ULTRASSECRETO, SECRETO ou RESERVADO no BAR, esse boletim deverá ser classificado no mesmo grau de sigilo do seu conteúdo.

§ 3º O BAR que for classificado não deverá conter assuntos com graus de sigilo distintos.

§ 4º Quando o BAR for classificado, deverá ser confeccionado o respectivo TCI.

§ 5º Aquele que obtiver acesso à informação, de que trata este artigo e o § 2º do art. 23, será responsabilizado por seu uso indevido.

§ 6º O pedido de acesso a informação pessoal deverá observar os procedimentos previstos nos art. 55 a 61 do Decreto nº 7.724, de 2012.

Seção II

Das Informações Referentes a Projetos de Pesquisa e Desenvolvimento Científico ou Tecnológico

Art. 31. A informação referente a projeto de pesquisa e desenvolvimento científico ou tecnológico, cujo sigilo seja imprescindível à segurança da sociedade ou do Estado, terá seu acesso

restrito a militar ou servidor que, devidamente autorizado, tenha a necessidade de conhecer seu conteúdo por força de atribuição funcional, independentemente de classificação de sigilo.

Art. 32. A restrição de acesso perdurará pelo período que for necessário à consecução desse projeto ou até que sua divulgação não possibilite vantagem de qualquer natureza a outra nação ou a empresa não envolvida no respectivo projeto.

Art. 33. A informação a que se refere o art. 31 deverá receber marcação nas partes superior e inferior de todas as suas páginas, existindo ou não classificação de sigilo, conforme modelo constante do Anexo C.

Seção III
Das Informações Contidas em Documentos Preparatórios

Art. 34. Para efeito destas IG, são exemplos de documentos preparatórios:

I – pareceres;

II – notas técnicas;

III – documentos operacionais, de pessoal ou de logística, tais como:

a) sumário e mensagem diária de operações;

b) mensagens operacionais; e

c) sumário ou mapa de situação de pessoal ou material;

IV – sindicância, inquérito policial militar, processo administrativo ou disciplinar, tomada de contas especial, prestação de contas anual e outros; e

V – documentos de inteligência.

Art. 35. Os documentos de inteligência, em virtude da possibilidade de conter dados sensíveis ou sigilosos, não devem:

I – ser utilizados como documentos integrantes de processos, de inquéritos, de sindicâncias, de documentos internos, de ofícios etc.;

II – ensejar quaisquer atividades, mesmo regulamentares, que coloquem em risco o seu sigilo e a proteção da fonte; e

III – ser usados com finalidade administrativa, disciplinar ou de qualquer natureza diversa da atividade de inteligência.

Art. 36. São exemplos de documentos de inteligência:

I – informe;

II – informação;

III – apreciação;

IV – estimativa;

V – relatório, mensagem e síntese de inteligência;

VI – levantamento estratégico de área;

VII – conjuntura e suas avaliações; e

VIII – demais documentos participantes do ciclo de produção do conhecimento de inteligência.

Art. 37. O acesso a documento preparatório ou a informação nele contida, utilizados como fundamento de tomada de decisão ou de ato administrativo, será assegurado a partir da edição do ato ou da decisão, conforme o art. 20 do Decreto nº 7.724, de 2012.

Parágrafo único. Enquanto o documento preparatório não for explicitamente referenciado em Documento Interno do Exército (DIEx), em ofício ou na edição de ato administrativo ou de decisão, o acesso será restrito somente a quem tenha necessidade funcional de conhecer ou quem possui credencial de segurança para acesso.

Art. 38. O documento preparatório deverá receber marcação na parte superior e inferior de todas as suas páginas, caso não haja outra condição de sigilo, conforme modelo do Anexo C.

Seção IV
Das Áreas e Instalações de Acesso Restrito

Art. 39. A área ou instalação que contenha documento ou material sigiloso que, por sua utilização ou finalidade, demandar proteção terá seu acesso restrito a militar ou servidor cadastrado e com a autorização do Cmt, Ch ou Dir da OM que sobre ela possui jurisdição.

Art. 40. Na área ou instalação de acesso restrito deverão ser fixadas placas indicativas, em local visível, conforme modelos constantes do Anexo C, de modo a possibilitar sua visualização por qualquer pessoa que tente abordá-la.

Seção V
Dos Materiais de Acesso Restrito

Art. 41. Para efeito destas IG, deve ser considerado material de acesso restrito qualquer matéria, produto, substância ou sistema que contenha, utilize ou veicule conhecimento ou informação classificada em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica cuja divulgação implique risco ou dano aos interesses da sociedade e do Estado, tais como:

I – equipamento, máquina, modelo, molde, maquete, protótipo, artefato, aparelho, dispositivo, instrumento, representação cartográfica, sistema e suprimento;

II – veículo terrestre, aquaviário e aéreo, suas partes, peças e componentes;

III – armamento e seus acessórios, munição, aparelho, equipamento, suprimento e insumo correlato;

IV – aparelho, equipamento, suprimento e/ou programa relacionado à tecnologia da informação e comunicações, inclusive à inteligência de sinais, de imagens e cibernética;

V – recurso criptográfico;

VI – explosivo, líquido e gás;

VII – manual ou cartilha de instrução;

VIII – plano de segurança de área ou instalação de acesso restrito;

IX – meio de armazenamento de dados ou informação sigilosa, tais como disco sonoro e óptico (CD-ROM e DVD), fita e disco magnético, **pen drive**, HD externos, cartão de memória e demais meios de armazenamento de dados (**smartphone** etc.);

X – credencial de segurança;

XI – BAR; e

XII – ativos de informação, sistemas, banco de dados e equipamentos dos canais de

comunicação seguros.

Art. 42. Todo material de acesso restrito deverá receber marcação (impressa ou fixada) prevista nos modelos constantes do Anexo C.

CAPÍTULO IV
DAS MEDIDAS DE CONTROLE

Seção I
Das Orientações Gerais

Art. 43. Compete ao Cmt, Ch ou Dir de OM manter o pessoal sob suas ordens atualizado sobre as medidas de controle da informação sigilosa em vigor.

Art. 44. Qualquer militar ou servidor, que tenha conhecimento de uma situação na qual uma informação sigilosa possa estar ou venha a ser comprometida, deverá informar tal fato ao seu Ch imediato e/ou à autoridade responsável pela proteção dessa informação.

Art. 45. Qualquer militar ou servidor, que tenha extraviado documento ou material sigiloso, deverá participar o fato imediatamente ao seu Ch imediato e/ou à autoridade responsável pela custódia.

Parágrafo único. Idêntica providência deverá ser tomada quando se encontre ou se tenha conhecimento que foi encontrado documento ou material sigiloso.

Art. 46. Constatando-se ocorrência que possa implicar no comprometimento de informação sigilosa, a autoridade competente tomará as providências necessárias para verificar a extensão do comprometimento e apurar responsabilidades.

Art. 47. Todo militar ou servidor, ao deixar o exercício de determinado cargo ou função, deverá passar ao seu substituto todo documento ou material classificado até então sob sua custódia, devidamente conferido.

Seção II
Do Acesso

Art. 48. Nos termos do art. 5º, inciso XXXIII, da Constituição Federal, de 1988, todo cidadão tem o direito a receber do órgão público informação de seu interesse particular, coletivo ou geral, que será prestada no prazo da lei, sob pena de responsabilidade, ressalvada aquela cujo sigilo seja imprescindível à segurança da sociedade ou do Estado.

Art. 49. Cabe ao Cmt, Ch ou Dir, no âmbito de sua OM, observadas as normas e procedimentos específicos aplicáveis, assegurar:

I – a gestão transparente da informação, propiciando seu amplo acesso e divulgação, seguindo as prescrições constantes nas normas vigentes que tratam do assunto; e

II – a proteção da informação sigilosa, observada a sua disponibilidade, autenticidade e integridade.

Art. 50. O acesso à informação classificada é estritamente funcional e independe de grau hierárquico do militar, sendo, contudo, obrigatório o credenciamento de segurança compatível, de acordo com as normas de credenciamento vigentes.

§ 1º O acesso de militar ou civil a documento, instalação ou material sob restrição de acesso exige a assinatura de Termo de Compromisso e Manutenção de Sigilo (TCMS), previsto no Anexo E destas IG, não havendo necessidade de concessão de credenciamento de segurança.

§ 2º Cabe ao Cmt, Ch ou Dir, no âmbito de sua OM, regular o acesso, considerando os seguintes aspectos:

I – necessidade do serviço;

II – necessidade de conhecer; e

III – nível de credenciamento.

Art. 51. O acesso a informação classificada por pessoa não credenciada ou não autorizada por legislação poderá ser permitido em caráter excepcional, mediante assinatura de TCMS, pelo qual a pessoa obrigar-se-á a manter sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

Art. 52. Os demais acessos previstos na legislação em vigor serão concedidos de acordo com o que prescreve a Lei nº 12.527, de 2011, a Lei nº 13.709, de 2018, o Decreto nº 7.845, de 2012, o Decreto nº 11.527, de 2023, e a legislação específica do Exército sobre o assunto.

Parágrafo único. Não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais.

Seção III
Dos Documentos e Materiais Controlados

Art. 53. O documento ou material classificado como ULTRASSECRETO deverá, por sua natureza, ser considerado DC ou MC.

Art. 54. Qualquer documento sigiloso ou material, a critério da autoridade que o produziu ou o classificou, deverá ser considerado como DC/MC.

Art. 55. Devido à sua natureza, o material criptográfico e/ou criptofônico deverá ser considerado sob restrição de acesso e MC, mesmo quando não seja classificado.

§ 1º Os manuais de equipamento criptográfico ou criptofônico deverão ser considerados MC.

§ 2º O sistema de cifra deverá ser guardado em local distinto de seus códigos.

Art. 56. O DC/MC, sempre que possível, deverá ser entregue pessoalmente ao seu destinatário, mediante assinatura de recibo. Caso o DC/MC seja classificado, a entrega deverá ser feita por pessoa credenciada.

Art. 57. Ao receber qualquer DC/MC, o detentor deverá verificar a integridade física do documento/material e, se for o caso, informar as alterações encontradas ao órgão controlador.

Art. 58. A responsabilidade pela custódia de DC/MC deverá ser atribuída:

I – nos comandos militares de área, cuja chefia do Estado-Maior seja cargo privativo de oficial-general, ao oficial por ele designado;

II – nos demais grandes comandos e grandes unidades, ao Chefe do Estado-Maior;

III – no ODG, nos ODS, nos órgãos de apoio e institutos subordinados, nos estabelecimentos de ensino e nas aditâncias, cuja chefia seja de cargo privativo de oficial-general, ao Chefe de Gabinete ou oficial por ele designado;

IV – nas demais aditâncias, aos adidos militares; e

V – nas demais OM e estabelecimentos de ensino, ao respectivo Cmt, Ch ou Dir.

Art. 59. Para a guarda e eliminação do DC/MC, deverá ser observado o previsto nos art.

104 e 111 destas IG.

Art. 60. Para facilitar o controle e preservar o sigilo, todo DC/MC receberá um título convencional, atribuído pelo órgão controlador e por meio do qual deverá ser processado.

§ 1º O título convencional será constituído pela abreviatura ou sigla do órgão controlador, seguida da sigla DC ou MC, do número sequencial do documento ou material, ano de sua expedição e número do exemplar ou de série.

Exemplos:

GCMTEX-CIE / DC-03/05 Exemplar Nº 15
CML/MC-27/12 Nº de série 140872ª

§ 2º Qualquer referência a um DC/MC em documento (remessa, termo de inventário, de custódia, de transferência de guarda e de eliminação, BAR, ofício, DIEx, etc.) deverá ser feita por intermédio do título convencional, sendo expressamente vedada a utilização correlacionada dos títulos real e convencional, qualquer que seja a classificação sigilosa do DC/MC.

§ 3º O título convencional deverá constar da capa, se houver, e em todas as páginas do DC.

Art. 61. Cabe ao Cmt, Ch ou Dir de OM designar qual divisão/seção terá a responsabilidade de exercer o controle sobre o(s) DC/MC, sendo que essa divisão/seção ficará encarregada de:

I – publicar, em BAR, observando o § 2º do art. 60 destas IG, o recebimento, recolhimento, transferência ou eliminação de um DC/MC, sem, contudo, caracterizar a sua inclusão em carga ou descarga;

II – atribuir os títulos convencionais, quando for o caso; e

III – confeccionar, conferir e remeter ao órgão controlador os termos de custódia, de transferência de guarda, de inventário ou de eliminação, quando for o caso.

Parágrafo único. Sempre que possível, a atribuição de controlar o DC/MC deverá recair sobre a divisão/seção com encargos no ramo da contrainteligência.

Art. 62. Ao receber um novo DC/MC, o detentor deverá remeter ao órgão controlador uma cópia do Termo de Custódia, conforme o Anexo J.

Art. 63. O detentor de DC/MC deverá remeter ao órgão controlador, até 30 de junho de cada ano, uma cópia do Termo de Inventário atualizado, conforme o Anexo A.

Art. 64. Sempre que houver a substituição do detentor indireto de DC/MC, esse deverá proceder à passagem de custódia dos DC/MC para o seu substituto e remeter ao órgão controlador o Termo de Transferência de Guarda de Documento e/ou Material Controlado, conforme o Anexo B.

Parágrafo único. O citado termo deverá ser confeccionado em 3 (três) vias, sendo que a primeira deverá ser remetida ao órgão controlador, acompanhada do Termo de Inventário atualizado, e as demais deverão ficar com o antigo e o novo detentor.

Art. 65. Os Termos de Inventário, de Transferência de Guarda e de Custódia não serão classificados e deverão receber a designação de “MATERIAL DE ACESSO RESTRITO”, sendo aposto o carimbo conforme os modelos constantes nos Anexos A, B e J.

Art. 66. Ao receber o Termo de Inventário, de Transferência de Guarda e/ou de Custódia, o órgão controlador deverá acusar o recebimento e fazer constar, na oportunidade, qualquer divergência encontrada.

Art. 67. Sempre que ocorrer furto, roubo ou extravio de DC/MC, o Cmt, Ch ou Dir de OM deverá instaurar uma sindicância a fim de apurar as causas e os responsáveis, levantar as medidas de segurança orgânica que deverão ser revistas ou implementadas, bem como tomar as medidas penais, civis e administrativas decorrentes.

§ 1º O órgão controlador poderá remeter um novo exemplar de DC, em substituição ao anteriormente distribuído, desde que a divulgação de seu conteúdo não tenha acarretado grave comprometimento da segurança da informação.

§ 2º Em se tratando de DC relativo a sistema de cifra e código, o órgão controlador deverá substituir todos os exemplares comprometidos.

Seção IV
Das Marcações de Sigilo

Art. 68. A marcação do grau de sigilo de um documento deverá constar de todas as suas páginas, observadas as seguintes formalidades:

I – a marcação será centralizada, no cabeçalho e no rodapé de cada página, em cor contrastante com a do documento, preferencialmente em vermelho, conforme modelo constante do Anexo C; e

II – somente deverá ser usada outra cor para assinalar a classificação sigilosa quando o documento não permitir que se obtenha o contraste desejado.

Art. 69. O esboço, desenho, fotografia, imagem digital, arquivo digital, multimídia, negativo ou **slide** sigiloso terá marcado seu grau de sigilo em local que possibilite sua reprodução, em todas as suas cópias.

Parágrafo único. O negativo ou **slide** de que trata este artigo, cuja falta de espaço impossibilite a sua marcação, será utilizado em condição que garanta a sua segurança e guardado em recipiente que exiba a classificação correspondente à do seu conteúdo ou da condição que permite o estabelecimento de restrições ao seu acesso.

Art. 70. A fotografia ou a reprodução de negativo, sem legenda, terão marcados os seus respectivos graus de sigilo ou a condição que permite o estabelecimento de restrição ao seu acesso, no seu verso e na sua embalagem.

Art. 71. O negativo em rolo contínuo, relativo a reconhecimento e a levantamento aerofotogramétrico, terá marcado o grau de sigilo correspondente ou a condição que permite o estabelecimento de restrição ao seu acesso, no início e no fim de cada rolo.

Art. 72. O microfilme e o filme cinematográfico sigiloso serão acondicionados de modo tecnicamente seguro, devendo a embalagem exibir a marcação do grau de sigilo correspondente ao seu conteúdo ou da condição que permite o estabelecimento de restrição ao seu acesso.

Art. 73. A marcação do grau de sigilo em mapa, carta e fotocarta deverá ser feita logo acima do título e na parte inferior, sem prejuízo das imagens registradas, mesmo que es~~t~~se arquivo esteja digitalizado.

§ 1º A carta, a fotocarta, o mosaico montado a partir de fotografias aéreas, as imagens digitais e os **shapes** vetorizados serão classificados em razão dos detalhes que revelem e não apenas da classificação atribuída às informações que lhes deram origem.

§ 2º A fim de salvaguardar os sistemas do EB, os bancos de dados que contenham geoinformação considerada imprescindível à segurança da sociedade ou do Estado, de acordo com os incisos I, VI e VII do art. 25 do Decreto nº 7.724, de 2012, deverão possuir classificação das respectivas

informações e restrição ao acesso, evitando condutas que se enquadrem nos incisos II e IV do art. 32 da Lei nº 12.527, de 2011.

CAPÍTULO V
DA SEGURANÇA DA INFORMAÇÃO

Seção I
Da Segurança do Pessoal

Subseção I
Da Segurança no Processo Seletivo

Art. 74. A avaliação de cargo ou função, com o objetivo de determinar o seu grau de sensibilidade, bem como a investigação de segurança, necessária para o desempenho de uma função ou cargo sensível, deverá estar de acordo com a norma para a concessão de credencial de segurança vigente.

Art. 75. A função ou cargo que trate sobre informação sigilosa deverá ser compartimentada, a fim de restringir o acesso, considerando a necessidade de conhecer.

Art. 76. O acesso de pessoal às áreas citadas nos art. 125, 126 e 127 destas IG deverá estar de acordo com a norma de concessão de credenciamento vigente.

Subseção II
Da Segurança no Desempenho da Função

Art. 77. O credenciamento para cargo ou função deverá ocorrer antes do início do seu desempenho e estar de acordo com a norma para concessão de credencial de segurança vigente.

Parágrafo único. O militar ou servidor que tiver sua credencial revogada, conforme a norma vigente, não poderá continuar a exercer cargo ou função que exija credenciamento de segurança.

Art. 78. Para as situações previstas no artigo anterior, o Cmt, Ch ou Dir de OM deverá considerar:

I – o comportamento e/ou a vulnerabilidade incompatíveis com o cargo ou função;

II – o descontentamento no desempenho da função;

III – as vulnerabilidades em relação a recrutamento e/ou aliciamento adversos; e

IV – a assinatura e publicação do TCMS em BAR.

Subseção III
Da Segurança no Desligamento da Função

Art. 79. Após o desligamento de um militar ou servidor de um cargo ou função que exija credenciamento de segurança, o Cmt, Ch ou Dir de OM deverá:

I – manter em banco de dados o endereço do ex-integrante, possibilitando o acompanhamento do militar ou do servidor que ocupava função sensível;

II – determinar o apagamento seguro de todas as pastas e arquivos temporários, por ele produzidos, no(s) computador(es) existente(s) na OM;

III – orientar ao ex-integrante que informe, de imediato, qualquer tentativa de cooptação de que venha a ser alvo; e

IV – informar ao militar ou servidor desligado que o sigilo das informações de que tomou conhecimento deverá ser mantido, de acordo com o TCMS assinado no início do desempenho da função, que permanecerá arquivado em guarda permanente pela OM.

Seção II
Da Segurança da Documentação

Subseção I
Das Medidas Gerais de Segurança da Documentação

Art. 80. As medidas de segurança da documentação previstas nestas IG devem ser adotadas para as atividades de produção, tramitação, classificação, acesso, uso, avaliação, arquivamento ou eliminação.

Art. 81. Medidas especiais de segurança devem ser adotadas para toda documentação sigilosa.

Parágrafo único. A publicação de ato normativo relativo à informação sigilosa, que possua sigilo legal, contratual ou judicial, poderá limitar-se, quando necessário, aos respectivos números, data de expedição ou ementas, redigidos de modo a não comprometer o seu sigilo.

Subseção II
Da Segurança na Produção

Art. 82. Todo documento preparatório, cuja posterior classificação seja visualizada, deverá ser marcado como "DOCUMENTO PREPARATÓRIO – ACESSO RESTRITO" já na sua produção, conforme modelo do Anexo C.

Parágrafo único. Após concluído, caso a informação contida no documento se enquadre nas condicionantes do art. 23 da Lei nº 12.527, de 2011, esse documento poderá ser classificado, recebendo seu grau de sigilo conforme procedimentos constantes dos art. 11 a 20 destas IG.

Art. 83. Embora partes de um documento (página, parágrafo, seção, parte componente ou anexo) possam merecer diferentes classificações, à sua versão completa será atribuído o grau de sigilo mais elevado.

Parágrafo único. Na hipótese de documento que contenha informações classificadas em diferentes graus de sigilo, fica assegurado o acesso à parte não classificada por meio de certidão, extrato ou cópia, com ocultação da parte sob restrição.

Art. 84. A classificação de um grupo de documentos, que formem um conjunto, deve ser a do documento de mais alta classificação que ele contenha.

Art. 85. O responsável pela produção de documento sigiloso deverá eliminar nota manuscrita, clichê, carbono, prova, cópia inservível ou qualquer outro elemento que possa dar origem a cópia não autorizada, do todo ou de parte do documento original.

Art. 86. Em todo o documento sigiloso, as páginas serão numeradas seguidamente, devendo cada uma conter, também, a indicação sobre o total de páginas que o compõe (exemplos: 5/9, 2/17 ou 1/39).

Art. 87. Sempre que a produção de documento sigiloso for efetuada em oficina gráfica, copiadora ou impressora instalada em local diferente daquele da produção, essa operação deverá ser acompanhada por militar ou servidor credenciado, que será o responsável pela garantia do sigilo durante essa atividade.

Subseção III
Da Segurança na Expedição e Recepção

Art. 88. O documento sigiloso poderá ser encaminhado fisicamente, obedecidas as seguintes prescrições:

I – é permitida a remessa por intermédio dos correios, desde que registrada;

II – é permitida a remessa por intermédio de mala diplomática; e

III – é permitida a remessa por intermédio de mensageiro, desde que credenciado para manipular/acessar documento classificado ou mediante assinatura do TCMS, no caso de/quando se tratar de documento com restrição de acesso.

§ 1º A expedição, a condução e a entrega de documento impresso, com informação classificada em grau de sigilo ULTRASSECRETO, será efetuada exclusivamente por mensageiro credenciado.

§ 2º O mensageiro deverá ser instruído sobre como proceder quando perceber qualquer tipo de ameaça ou incidente que possa resultar em comprometimento do sigilo do documento ou do material transportado.

Art. 89. Na expedição do documento impresso sigiloso deverão ser observadas as seguintes prescrições:

I – o documento a ser expedido deverá ser acondicionado em envelope duplo;

II – o envelope externo deverá conter apenas a função do destinatário e seu endereço, sem qualquer anotação que indique o grau de sigilo ou o motivo da restrição de acesso ao seu conteúdo;

III – no envelope interno deverá ser inscrito o nome e a função do destinatário, o seu endereço e o grau de sigilo ou motivo da restrição de acesso ao conteúdo do documento, de modo a ser visto logo que removido o envelope externo;

IV – o envelope interno deverá ser lacrado e o documento sigiloso deverá estar acompanhado de um recibo; e

V – o recibo destinado ao controle da expedição/recepção e da custódia do documento sigiloso deverá conter indicações sobre o remetente, o destinatário, o número ou outro indicativo que identifique o documento.

Art. 90. O expediente que encaminha documento classificado ou sua cópia não será classificado, desde que não contenha frações significativas desse documento ou cópia.

§ 1º Como medida complementar de segurança para o trâmite e manuseio desse tipo de expediente, deverá constar no campo “assunto”, em vermelho, ou, quando não for possível a impressão colorida, em negrito, um dos seguintes textos: “encaminhamento de DOCUMENTO CLASSIFICADO” ou “encaminhamento de DOCUMENTO SOB RESTRIÇÃO DE ACESSO”.

§ 2º O trâmite eletrônico desses documentos será feito conforme o previsto no art. 130 destas IG.

Art. 91. Quando for necessário que somente o destinatário tome conhecimento do assunto tratado, o envelope interno deverá conter, além do nome do destinatário, a inscrição "PESSOAL", precedendo a indicação da restrição ou classificação, quando houver.

Parágrafo único. Para documento oficial, com NUP/NUD, a situação de documento “PESSOAL” será temporária e restrita a quem terá o primeiro acesso ao seu conteúdo.

Art. 92. Providências adicionais poderão ser adotadas pelo Cmt, Ch ou Dir de OM, visando aumentar a segurança na expedição de documento sigiloso.

§ 1º A expedição e o recebimento de documento sigiloso deverão ser registrados em livro protocolo (controle de saída ou controle de entrada), próprio para esses documentos.

§ 2º O documento classificado expedido deverá ser enviado obrigatoriamente com o TCI.

§ 3º O documento classificado expedido deverá ser registrado no sistema de cadastro e controle de documentos classificados da OM em até 90 (noventa) dias após a expedição.

Art. 93. O responsável pelo serviço de correio, ou qualquer militar ou servidor, quando constatar que a correspondência recebida é um documento sigiloso, deverá encaminhá-la à divisão/seção que tiver sob seu encargo a atividade de inteligência, para despacho da autoridade competente.

Art. 94. Após despacho da autoridade competente, deverá ser confeccionado um registro de todos os dados identificadores da divisão/seção por onde tramitou ou para qual foi distribuído o documento sigiloso, além do militar ou servidor que teve acesso à documentação.

Parágrafo único. Além do efeito de protocolo, o registro indicará a tramitação e o responsável pela custódia do documento.

Art. 95. Ao responsável pelo recebimento de documento sigiloso incumbe:

I – verificar e registrar, se for o caso, indícios de violação ou de qualquer irregularidade na correspondência recebida, dando ciência do fato ao destinatário, o qual informará o remetente; e

II – proceder ao registro do documento e ao controle de sua tramitação, conforme previsto no art. 94 destas IG.

Art. 96. Recebido o documento sigiloso impresso, seu recibo anexado deverá ser assinado e datado pelo destinatário e devolvido ao remetente.

Parágrafo único. A remessa do recibo não deve ser feita com características de sigilo.

Art. 97. O destinatário de documento impresso sigiloso deverá comunicar ao remetente qualquer indício de violação do documento, tal como rasuras e irregularidades de impressão ou de paginação.

Subseção IV
Da Segurança no Manuseio

Art. 98. O documento sigiloso somente poderá ser manuseado por pessoa credenciada, que tenha necessidade de conhecer seu conteúdo e esteja autorizada pelo Cmt, Ch ou Dir da OM.

Parágrafo único. Para tal, deve-se correlacionar o grau de sigilo com a categoria da credencial de segurança de quem manuseará o documento classificado.

Art. 99. Todo documento sigiloso deverá ser manuseado pelo menor número possível de pessoas, a fim de tornar mais efetiva a sua segurança.

Art. 100. Poderá ser elaborada cópia ou extrato de documento sigiloso, mediante consentimento expresso:

I – da autoridade classificadora, para documento no grau de sigilo ULTRASSECRETO;

II – da autoridade classificadora ou autoridade hierarquicamente superior, para documento no grau de sigilo SECRETO e RESERVADO; e

III – da autoridade destinatária, para documento sob restrição de acesso, exceto quando expressamente vedado no próprio documento.

Parágrafo único. A cópia será autenticada pela autoridade que a autorizou.

Art. 101. A confecção de cópia de documento sigiloso deverá ser limitada ao estritamente necessário.

§ 1º A cópia do documento classificado deverá conter cópia do respectivo TCI.

§ 2º Em toda cópia de documento sigiloso deverá constar a marcação de alerta para sua destruição, conforme o previsto no Anexo C.

Art. 102. A cópia ou o extrato de documento sigiloso deverá receber um código numérico ou alfanumérico específico para cada destinatário, a fim de identificar a origem de um possível vazamento e facilitar o seu controle.

§ 1º O código citado no **caput** deverá ser colocado no corpo do texto, em cada página do documento, sendo visível e de fácil identificação em qualquer reprodução gráfica realizada, conforme modelo constante do Anexo G.

§ 2º No documento original deverá constar a relação de todos os destinatários com os seus respectivos códigos.

Art. 103. O responsável pela cópia de documento sigiloso deverá destruir a cópia inservível ou qualquer outro elemento que possa dar origem à cópia não autorizada do todo ou de parte do documento original.

Art. 104. Sempre que a cópia de documento sigiloso for efetuada em copiadora ou em impressora instalada em local diferente daquele onde foi produzido o documento original, essa operação deverá ser acompanhada por militar ou servidor credenciado, que será o responsável pela garantia do sigilo durante essa atividade.

Art. 105. À cópia ou ao extrato de documento sigiloso será atribuída a classificação ou a situação de restrição de acesso igual àquela atribuída ao documento que lhe deu origem.

Parágrafo único. Para isso, os seguintes procedimentos deverão ser adotados:

I – a cópia deverá receber marcação adequada, em cor contrastante com a do documento, preferencialmente em vermelho, conforme modelo constante do Anexo C; e

II – no corpo do documento que deu origem à cópia, deverá constar o número e o destinatário dessa.

Subseção V
Da Segurança no Arquivamento

Art. 106. O documento sigiloso deverá ser guardado em condições especiais de segurança.

§ 1º Para a guarda de documento no grau de sigilo ULTRASSECRETO, é obrigatório, no mínimo, o uso de cofre com segredo de 3 (três) combinações ou material que ofereça segurança equivalente ou superior, instalado de forma fixa em uma dependência com controle de acesso.

§ 2º Na impossibilidade de se adotar o disposto no parágrafo anterior, o documento no grau de sigilo ULTRASSECRETO deverá ser mantido sob guarda armada.

§ 3º Para a guarda de documento no grau de sigilo SECRETO, é obrigatório seu armazenamento em cofre e, se possível, a adoção de medidas de segurança idênticas àquelas adotadas

para aqueles com o grau ULTRASSECRETO.

§ 4º Para a guarda de documento no grau de sigilo RESERVADO ou sob outra restrição, é obrigatório, no mínimo, o uso de arquivo com chave, fixado em uma dependência com controle de acesso.

§ 5º Não deverá estar guardado no mesmo cofre ou arquivo o texto em claro e o seu correspondente criptografado.

Art. 107. É obrigatório que os detentores de documentação sigilosa estabeleçam procedimentos relativos à sua evacuação, em situações de emergência.

§ 1º Os documentos sigilosos produzidos no exterior deverão ser trazidos para o Brasil, por ocasião do término da missão.

§ 2º Os responsáveis pelas missões no exterior devem planejar a destruição de documentos sigilosos, quando não for possível a transferência de custódia para OM em território nacional, especialmente quando for verificada a possibilidade de ocorrer acesso não autorizado.

§ 3º A destruição ocorrerá mediante autorização de autoridade competente.

§ 4º Em caso de ordem de evacuação de embaixada, a autoridade que determinar a retirada dos funcionários e materiais será aquela que autorizará a destruição.

§ 5º A medida prevista no **caput** requer o estabelecimento de prioridades e de responsabilidades e a determinação antecipada de local alternativo para abrigar os documentos a serem salvos.

Subseção VI
Da Segurança na Eliminação

Art. 108. O original do documento classificado deverá ser mantido em arquivo e submetido, dentro do período previsto, à apreciação da respectiva comissão ou subcomissão responsável pela avaliação de documentos.

Art. 109. O original da informação com grau de sigilo ULTRASSECRETO ou SECRETO, mesmo após desclassificado, é de guarda permanente, devendo ser preservado de acordo com o art. 39 do Decreto nº 7.724, de 2012.

Parágrafo único. A cópia de documento com grau de sigilo ULTRASSECRETO ou SECRETO, após desclassificado, caso destituída de valor para fins de arquivo e/ou consulta, poderá ser eliminada tão logo se torne inservível, seguindo-se o que prescrevem as normas sobre gestão documental do Exército.

Art. 110. O documento original com grau de sigilo RESERVADO, após desclassificado e se avaliado como destituído de valor para fins de arquivo ou consulta, poderá ser eliminado tão logo se torne inservível, seguindo-se o que prescrevem o art. 108 destas IG e as normas sobre gestão documental.

Parágrafo único. A via do documento expedida com grau de sigilo RESERVADO, após ter sido desclassificada pela comissão ou subcomissão responsável pela avaliação de documentos da OM expedidora e destituída de valor para fins de arquivo ou consulta, deverá ser eliminada.

Art. 111. Para a eliminação de documento com informação sob restrição de acesso, deverá ser seguido o que prescrevem as normas sobre gestão documental em vigor.

Art. 112. Para a eliminação de exemplar de DC, deverá ser seguido o que prescrevem as normas sobre gestão documental e deverão ser observados os seguintes procedimentos:

I – a autoridade que classificou o original deverá determinar o recolhimento do exemplar que será eliminado;

II – após certificar-se de que o original foi mantido em arquivo, deverá ser lavrado o respectivo Termo de Eliminação do exemplar de DC, conforme modelo constante do Anexo D, assinado pela autoridade que classificou o original e por 2 (duas) testemunhas;

III – o termo citado no inciso anterior deverá ser publicado em BAR; e

IV – deverão ser lançados, no verso da primeira folha do DC original, o número e a data do BAR que publicou o Termo de Eliminação do exemplar.

Parágrafo único. Toda publicação ou referência a DC deverá atender ao § 2º do art. 60 das presentes IG.

Art. 113. No caso de impossibilidade de recolhimento do DC/MC, nos termos do inciso I do art. 112, o exemplar inservível de DC deverá ser eliminado pela autoridade que mantém a custódia.

Parágrafo único. Para tanto, a autoridade custodiante e a autoridade controladora devem adotar os seguintes procedimentos:

I – autoridade controladora:

a) informar à OM que mantém a custódia do DC que proceda à eliminação e à publicação em BAR do Termo de Eliminação, conforme modelo constante do Anexo D;

b) solicitar a remessa de exemplar do Termo de Eliminação e da folha do BAR que publicou o ato à autoridade controladora;

c) manter o original do DC arquivado; e

d) manter o controle da eliminação de exemplares e de seus respectivos termos, arquivando os Termo de Eliminação, acompanhados do DC original;

II – autoridade custodiante de DC:

a) eliminar o DC de acordo com as orientações da autoridade controladora;

b) confeccionar o Termo de Eliminação e publicá-lo em BAR; e

c) remeter cópia do Termo de Eliminação e da cópia da folha de BAR que publicou a eliminação à autoridade controladora.

Seção III
Da Segurança do Material

Subseção I
Das Medidas Gerais de Segurança do Material

Art. 114. A segurança do material sigiloso adotará as mesmas prescrições estabelecidas para a documentação, no que for aplicável.

Art. 115. O Cmt, Ch ou Dir, particularmente de órgão técnico ou estabelecimento de ensino, responsável por programa de pesquisa ou por projeto para o qual julgar conveniente manter sigilo sobre determinado material ou suas partes, deverá providenciar para que seja atribuída a restrição de acesso correspondente a esse material.

Parágrafo único. Aplica-se o disposto neste artigo ao Ch ou Dir de órgão encarregado da fiscalização e do controle de atividades de empresa vinculada ou privada, para fins de desenvolvimento, produção e/ou exportação de material de interesse da defesa nacional.

Art. 116. A empresa vinculada ou privada, desenvolvedora de pesquisa ou projeto de interesse nacional que contenha material sob restrição de acesso enquadrado em um dos incisos do art. 23 da Lei nº 12.527, de 2011, deverá providenciar a classificação desse material, mediante entendimento com o órgão a que estiver ligado, para efeito daquela pesquisa ou projeto.

Art. 117. O Cmt, Ch, Dir ou titular de órgão técnico, estabelecimento de ensino ou de empresa vinculada, encarregada da preparação de plano, pesquisa, trabalho de aperfeiçoamento, projeto de pesquisa e desenvolvimento, prova, produção, aquisição, armazenagem ou emprego de material sigiloso, é o responsável pela expedição das instruções adicionais que se tornarem necessárias à salvaguarda das informações relacionadas com esse material .

Art. 118. A informação sigilosa concernente a programa técnico ou aperfeiçoamento de material só deverá ser fornecida ao militar, servidor, pesquisador ou empresa que, por sua função oficial ou contratual, a ela deva ter acesso.

§ 1º Em nenhuma hipótese, a informação sigilosa será controlada ou coordenada por pessoa jurídica de direito privado.

§ 2º O órgão responsável pelo desenvolvimento de pesquisa ou projeto de interesse nacional deverá controlar e coordenar o fornecimento de informação sigilosa a pessoa física ou jurídica envolvida nessa atividade.

Art. 119. Em demonstração, exposição ou exibição para pessoas integrantes da Instituição, cabe ao Cmt, Ch ou Dir da OM responsável tomar as medidas de segurança necessárias com o material exposto que esteja sob restrição de acesso, bem como no que tange à divulgação das suas características técnicas.

Parágrafo único. Não é autorizada a demonstração, exposição ou exibição de material que esteja sob restrição de acesso a pessoas não integrantes da Instituição, salvo as que tenham necessidade de conhecer e que tenham a devida autorização para o acesso.

Art. 120. É vedado o registro de imagem de material sigiloso no âmbito do EB. Em casos especiais, esse registro poderá ser autorizado pelo Cmt, Ch ou Dir de OM responsável por sua custódia.

§ 1º O registro de imagem somente poderá ser feito mediante a definição prévia de sua futura utilização.

§ 2º O registro de imagem somente poderá ser utilizado após ser analisado pelo comando, chefia ou direção que o autorizou.

§ 3º O registro de imagem de material classificado deve observar o mesmo tratamento para documento classificado, como prescrito no art. 100 destas IG, e ser realizado por pessoa que possua a credencial de segurança específica.

§ 4º Ao registro de imagem de material classificado será atribuído grau de sigilo igual ao do material que lhe deu origem.

§ 5º O registro de imagem de material sob restrição de acesso deverá ser concedido mediante assinatura do TCMS.

Art. 121. É vedado o registro de imagem de material sigiloso ou de processo de fabricação considerado sigiloso conduzido por empresa civil. Em casos especiais, esse registro poderá ser autorizado pelo ODS responsável pelo desenvolvimento da pesquisa ou projeto, mediante solicitação da chefia do segmento técnico responsável.

§ 1º O registro de imagem somente poderá ser feito mediante a definição prévia de sua futura utilização.

§ 2º O registro de imagem somente poderá ser utilizado após ser analisado pelo

comando, chefia ou direção que o autorizou.

§ 3º O registro de imagem de material classificado deve observar o mesmo tratamento para documento classificado, como prescrito no art. 102 destas IG, e ser realizado por pessoa que possua a credencial de segurança específica.

§ 4º Ao registro de imagem de material classificado, ativos de informação ou de processo de fabricação considerado sigiloso será atribuído grau de sigilo igual ao do material que lhe deu origem.

§ 5º O registro de imagem de material sob restrição de acesso deverá ser concedido mediante assinatura do TCMS.

Subseção II
Da Segurança no Transporte

Art. 122. A definição do meio de transporte e do nível de segurança a ser utilizado para deslocamento de material sigiloso é de responsabilidade do detentor da sua custódia, que deverá considerar o grau de sigilo atribuído ao respectivo material, a extensão do percurso e o grau de risco do itinerário a ser percorrido.

Parágrafo único. O material sigiloso poderá ser transportado por empresa contratada para tal fim, devendo as medidas necessárias para a segurança do material serem estabelecidas e executadas por pessoa credenciada ou com permissão de acesso, consignando-se as condições em cláusulas contratuais específicas.

Art. 123. Caso a distância de transporte, o seu tamanho e a sua quantidade permitirem, o material sigiloso deverá ser entregue pessoalmente ao destinatário, por pessoa credenciada ou com permissão de acesso, mediante assinatura de recibo.

Art. 124. A critério da autoridade competente, poderão ser empregados guardas armados, civis ou militares, no transporte de material sigiloso.

Subseção III
Da Segurança na Eliminação de Material Controlado

Art. 125. Para a eliminação de MC, deverão ser obedecidas as seguintes prescrições:

I – somente o órgão controlador poderá autorizar a eliminação;

II – deverá ser lavrado o respectivo Termo de Eliminação de Material Controlado, conforme modelo constante do Anexo H, assinado pelo detentor e por 2 (duas) testemunhas;

III – o Termo de Eliminação citado no inciso anterior deverá ser publicado no BAR da OM custodiante;

IV – após a eliminação, a autoridade custodiante deverá encaminhar cópia do Termo de Eliminação e cópia da(s) folha(s) do boletim no qual foi publicada ao órgão controlador, que deverá transcrever essa publicação em seu BAR; e

V – o método utilizado para a destruição deverá assegurar a desintegração do MC.

Parágrafo único. Para os demais materiais e produtos, deverão ser obedecidas as normas de controle dos respectivos órgãos gestores.

Seção IV
Da Segurança das Áreas e Instalações

Art. 126. Caberá ao Cmt, Ch ou Dir a definição, a demarcação, a sinalização, a segurança e a concessão de acesso à área restrita, no âmbito de sua OM (seção, divisão, departamento etc.).

§ 1º Para tanto, deverá ser elaborada norma de controle de acesso às áreas restritas, com a finalidade de normatizar procedimentos.

§ 2º As áreas de inteligência, tecnologia da informação, jurídica, cibernética, comunicações, ciência e tecnologia, guerra eletrônica e as consideradas vitais para o pleno funcionamento da OM, tais como reserva de armamento, paiol, caixa d'água, central elétrica, entre outras, deverão ser consideradas de acesso restrito.

§ 3º A norma de controle de acesso, citada no **caput** deste artigo, deverá contemplar a proibição da entrada de pessoas conduzindo máquina fotográfica, filmadora, celular, gravador ou qualquer meio de captura de imagens e sons em área e instalação em que seja armazenado documento ou material sigiloso, sem a autorização expressa do Cmt, Ch ou Dir.

§ 4º Para efeito deste artigo, não é considerado visitante o agente público ou o particular que, oficialmente, execute atividade pública diretamente vinculada à elaboração de estudo ou trabalho considerado sigiloso.

Art. 127. A área ou instalação de acesso restrito deverá ser indicada, por intermédio de placa(s) afixada(s) na(s) parede(s) externa(s), de forma destacada, preferencialmente na cor vermelha, principalmente junto à(s) entrada(s), conforme modelo constante do Anexo C.

Parágrafo único. Tal marcação tem por finalidade precípua apresentar-se como um primeiro elemento dissuasor ao comprometimento ou à quebra de segurança.

Art. 128. As instalações das OM, particularmente as de tecnologia da informação, de cibernética, de guerra eletrônica e de comunicações, deverão utilizar rede elétrica dimensionada ao número de equipamentos a ela ligados, visando à sua proteção contra sobrecargas.

Parágrafo único. Igual procedimento deverá ser adotado quanto a para-raios e aterramento adequado, visando à proteção contra descargas atmosféricas.

Seção V
Da Segurança das Comunicações

Subseção I
Das Medidas Gerais de Segurança das Comunicações

Art. 129. A comunicação de dados, de qualquer natureza, deverá ser realizada por rede de telecomunicações e por serviço de tecnologia da informação fornecido por órgão ou entidade da administração pública federal, incluindo empresa pública e sociedade de economia mista da União e suas subsidiárias.

§ 1º O disposto no **caput** não se aplica às comunicações realizadas por meio de serviço móvel pessoal e serviço telefônico fixo comutado.

§ 2º Os ativos de informação, programa ou equipamento destinado à atividade de que trata o **caput** deverão ter características que permitam a auditoria para fins de garantia da disponibilidade, da integridade, da confidencialidade e da autenticidade das informações.

§ 3º O armazenamento e a recuperação de dados a que se refere o **caput** deverão ser realizados em centro de processamento de dados fornecido por órgão ou entidade da administração pública federal.

Subseção II

Da Segurança na Remessa ou Transmissão

Art. 130. A segurança na remessa ou transmissão de informação sigilosa é de responsabilidade de todo aquele que a manusear para tal fim.

Parágrafo único. As medidas de segurança deverão ser tomadas de acordo com as restrições de acesso necessárias e o meio de remessa ou transmissão utilizado.

Art. 131. A transmissão de informação classificada poderá ser realizada por meio eletrônico, desde que obrigatoriamente criptografado, em sistema de cifra de alta confiabilidade, com algoritmo de Estado, dentro da rede corporativa, por meio de canal seguro, como forma de mitigar o risco de quebra de segurança.

Parágrafo único. A informação sob restrição de acesso que trate de assunto de inteligência, de emprego de tropa ou de apoio logístico, particularmente as de transporte de munição e de armamento, deverá seguir o prescrito no **caput** deste artigo.

Art. 132. Na escolha do meio de transmissão eletrônica a ser utilizado, deverão ser priorizados os meios integrantes das diversas redes do EB.

Art. 133. Na ligação telefônica ou via fax, deve-se considerar a extrema vulnerabilidade desses meios para o trato de informação sigilosa.

§ 1º Na impossibilidade de utilização de outro meio mais seguro, deverá ser utilizado equipamento dotado de criptofonia ou criptografia.

§ 2º É proibida a utilização de fax sem a necessária confirmação do destinatário antes da transmissão do documento, evitando-se, dessa maneira, a recepção do documento por pessoa não autorizada.

Art. 134. Outros procedimentos relativos à segurança da transmissão deverão estar de acordo com os manuais para exploração dos meios de comunicações em vigor, desde que compatíveis com os preceitos da legislação específica que trata da segurança da informação sigilosa.

Subseção III
Da Segurança do Conteúdo

Art. 135. Todo documento criptografado recebido deverá ser tratado como estando sob restrição de acesso.

Art. 136. É proibida a utilização de qualquer sistema de cifra e código ou material criptográfico, em uso no EB , para o preparo de mensagem que não trate de assunto de serviço.

Art. 137. As tecnologias empregadas na segurança dos ativos de informação, em uso no EB , deverão ser consideradas sob restrição de acesso.

Seção VI
Da Segurança da Tecnologia da Informação e Comunicações

Subseção I
Da Segurança do Equipamento

Art. 138. A manutenção em ativos de informação deverá ser, preferencialmente, executada pelo pessoal especializado em equipamento informatizado da própria OM.

§ 1º Esgotados os meios da OM para a resolução de problemas de manutenção, a empresa de manutenção contratada deverá subordinar-se ao previsto no art. 51 destas IG.

§ 2º Qualquer serviço a ser executado por empresa contratada em equipamento de tecnologia da informação e comunicação (TIC), que contenha assunto sigiloso, deverá ser acompanhado pelo responsável por sua utilização.

§ 3º O computador que contenha informação sigilosa e que necessite de manutenção fora da OM deverá ter o seu disco rígido retirado e guardado em um cofre.

Subseção II
Da Segurança do Software

Art. 139. Deverá ser utilizado apenas o **software** licenciado de acordo com a legislação em vigor ou de domínio público, após parecer favorável e assessoramento técnico de pessoal especializado da divisão ou seção de tecnologia da informação da OM.

Parágrafo único. A instalação de **software** somente deverá ser realizada por pessoal habilitado da divisão/seção de tecnologia da informação existente na OM.

Art. 140. Deverá ser instalado e atualizado, periodicamente, um sistema antivírus fornecido pelo EB, com o objetivo de se evitar a disseminação de programas maliciosos nas redes de informática.

Subseção III
Da Segurança Física

Art. 141. Todo arquivo digital que contenha informação classificada deverá possuir cópia de segurança.

Art. 142. O original de programa em uso e a(s) cópia(s) de segurança de arquivo digital, contendo informação classificada, deverão estar armazenados em cofre fixado em uma dependência com restrição de acesso, localizada fora da divisão/seção de tecnologia da informação.

Art. 143. Além do previsto no art. 128 e seu parágrafo único, a divisão/seção de tecnologia da informação deverá utilizar, sempre que possível, gerador ou outro equipamento que garanta a continuidade no fornecimento de energia elétrica aos equipamentos de TIC.

Subseção IV
Da Segurança na Rede Mundial de Computadores

Art. 144. Deverá ser seguido o que prescrevem as Instruções Gerais para Utilização da Rede Mundial de Computadores pelo Exército Brasileiro (EB10-IG-01.010).

Art. 145. Os portais das OM, dos militares da ativa, da reserva ou dos servidores civis, bem como os computadores que estiverem conectados à Rede Mundial de Computadores ou a outras redes com acesso remoto, não deverão conter informação sigilosa.

Parágrafo único. Para fins deste artigo, serão considerados como informações da OM sob restrição de acesso, as abaixo especificadas:

I – vista aérea;

II – fotografias internas de pontos importantes (paiol, reserva de armamento etc.);

III – peculiaridades do seu emprego;

IV – características técnicas de sistema e/ou material de emprego militar;

V – informações pessoais dos seus integrantes; e

VI – informações contidas nos quadros de organização ou de material, entre outras.

Subseção V
Da Segurança no Correio Eletrônico, da Mensageria Eletrônica e do Armazenamento de Arquivo em Nuvem

Art. 146. Em caso de utilização de serviço de correio eletrônico, deverão ser adotados aqueles autorizados pelo Departamento de Ciência e Tecnologia para o trâmite de mensagens relacionadas ao serviço, sendo, preferencialmente, os fornecidos pelo EB.

Parágrafo único. É vedada a tramitação de informações sigilosas em serviços de correio eletrônico.

Art. 147. O correio eletrônico de procedência desconhecida não deverá ser aberto utilizando-se computador ligado à rede de informática da OM, principalmente o que contenha arquivo anexado.

Art. 148. A certificação digital deverá ser utilizada com o objetivo de permitir a autenticação e identificação da autoria de mensagem remetida via correio eletrônico.

Art. 149. É vedada a tramitação de informações sigilosas em serviços de mensageria eletrônica, ainda que esses serviços sejam autorizados ou fornecidos pelo Exército.

Art. 150. É vedada a utilização de serviços de armazenamento em nuvem de arquivos que contenham informações sigilosas, ainda que esses serviços sejam autorizados ou fornecidos pelo Exército.

Subseção VI
Da Segurança em Sistemas Corporativos, Intranet e Redes Locais

Art. 151. Deverá ser estabelecida senha de acesso para cada usuário aos sistemas e ambientes de rede, individual e intransferível, a qual deverá ser trocada frequentemente, para dificultar o acesso por pessoa não autorizada.

Art. 152. O controle de acesso lógico deverá ser restrito, em diferentes níveis, de acordo com a necessidade de conhecer de cada usuário do sistema.

Art. 153. A operação de inclusão, pesquisa, alteração e exclusão de dados nos sistemas corporativos deverá ser realizada por pessoa devidamente credenciada a acessar os diferentes níveis de administração do sistema.

Art. 154. Toda rede de OM, conectada ou não à Rede Mundial de Computadores, deverá possuir ferramenta ou sistema capaz de rastrear e identificar a origem e o responsável pelo acesso à rede e de dificultar o acesso à pessoa não credenciada.

Art. 155. Toda rede de OM, conectada ou não à Rede Mundial de Computadores, deverá possuir ferramenta ou sistema específico, sempre atualizado, capaz de rastrear e emitir relatório sobre pontos vulneráveis que poderão ser utilizados como porta de entrada para invasão nos sistemas dessa rede.

Art. 156. Nenhum computador que pertença à rede da OM e contenha informação classificada poderá ser conectado, mesmo que eventualmente, à Rede Mundial de Computadores ou a qualquer outra rede de acesso remoto.

Parágrafo único. Para um controle mais eficaz, tal computador não deverá ter a placa de fax-modem e deverá ter desabilitado ou bloqueado o recurso de conexão remota (sem fio).

Art. 157. A pasta digital, sem restrição de acesso ao público interno, normalmente disponível em redes das OM e nomeada “Pública”, não deverá ser utilizada para armazenamento de arquivo que contenha informação sigilosa.

Art. 158. Caso seja necessário o uso de dispositivo de armazenamento portátil (**pen drive**, cartão de memória etc.) em máquina utilizada por sistema corporativo, **intranet** e rede local, esse dispositivo deverá ser do tipo institucional, padronizado em cor e tamanho, identificado e etiquetado com orientações sobre seu uso, o que diminui significativamente o risco de comprometimento ou de propagação de vírus.

Parágrafo único. É vedado o uso de dispositivo de armazenamento móvel particular.

Subseção VII
Da Segurança contra Furto, Roubo ou Extravio de Dados

Art. 159. Não deverá ser utilizado computador pessoal para o trato de informação sigilosa de cunho funcional, considerando:

I – que o arquivo apagado do seu disco rígido poderá ser recuperado por pessoa não autorizada, com a utilização de programa específico; e

II – que a segurança do equipamento é relativa, levando-se em conta a possibilidade de ocorrência de imprevisto por ocasião do seu transporte.

Art. 160. Antes de ausentar-se do seu local de trabalho, mesmo que de forma breve, o usuário deverá fechar todos os programas acessados.

Art. 161. Cuidados especiais deverão ser adotados por ocasião da realização de instrução ou palestra, que trate de informação sigilosa, fora do ambiente normal de trabalho.

§ 1º Sempre que possível, deverá ser evitada a utilização do disco rígido para armazenar o conteúdo da palestra ou instrução, pois mesmo após apagado o arquivo que a contém, essa poderá ser recuperada por pessoa não autorizada, por meio do emprego de programa específico.

§ 2º A autorização para a confecção de cópia da palestra ou instrução, em **pen drive**, CD/DVD ou outro meio de armazenamento é da exclusiva responsabilidade de quem a proferiu ou ministrou.

Art. 162. Após a remessa ou transmissão de documento eletrônico que contenha informação sigilosa, deverá ser confeccionada uma cópia em dispositivo de armazenamento portátil, devendo essa cópia ser guardada em local seguro.

Parágrafo único. Quando for inevitável o transporte de informação sigilosa, esse procedimento deverá ser realizado em equipamento portátil (**notebook**, **tablet**, disco rígido externo etc.) fornecido pela OM, sendo que, para tal transporte, deverá ser utilizado programa que crie um **container** seguro.

Seção VII
Das Prescrições Diversas

Art. 163. A segurança da informação é responsabilidade de todos, mas, por envolver aspectos técnicos, é incumbência da divisão/seção com encargos no ramo de contrainteligência, que, com o auxílio das demais divisões/seções, deverá:

I – implementar o processo de desenvolvimento de contrainteligência da OM, mantendo-o atualizado;

II – realizar auditorias frequentes, a fim de levantar vulnerabilidades nas redes instaladas, acessos indevidos, tentativas de acesso, entre outros aspectos julgados pertinentes; e

III – aplicar, periodicamente, a lista de verificação de segurança orgânica, divulgando seus resultados por intermédio de um relatório, o qual deverá ser apresentado ao Cmt, Ch ou Dir e publicado em BAR, para a melhoria do nível de segurança da OM.

CAPÍTULO VI
DA CELEBRAÇÃO DE CONTRATOS

Art. 164. A entidade privada com previsão de assinatura de contrato sigiloso deverá ser habilitada para tal, conforme a norma de concessão de credenciamento vigente.

Art. 165. Observadas as normas gerais para licitação e contratação, estabelecidas pela Lei nº 14.133, de 1º de abril de 2021, e demais previsões da legislação, a celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção, cujo conteúdo seja sigiloso, é condicionada à assinatura de TCMS e ao estabelecimento de cláusulas contratuais que prevejam os seguintes requisitos:

I – conhecimento do aviso do edital e/ou do edital propriamente dito, permitido somente após a assinatura do termo citado no **caput**;

II – obrigação de manter o sigilo relativo ao objeto e sua execução;

III – possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;

IV – obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;

V – identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso a informação classificada e a material de acesso restrito;

VI – obrigação de receber inspeções para habilitação de segurança e sua manutenção;

VII – responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte; e

VIII – responsabilidade penal, civil e administrativa em caso de vazamento de informação (ões) sigilosa(s).

Art. 166. Ao órgão contratante ou que celebre convênio caberá providenciar para que o seu representante ou fiscal adote as medidas necessárias, de acordo com as prescrições contidas nestas IG, para a segurança do documento e/ou material sigiloso em poder do seu contratado, subcontratado, conveniado, subconveniado ou em curso de fabricação em suas instalações.

Art. 167. Comprovado o vazamento de informação sigilosa que esteja enquadrada nos incisos I ao VIII do art. 25 da Lei nº 12.527, de 2011, haverá investigação visando à responsabilização penal, civil e administrativa de parte contratada, principalmente em relação a ativos de informação e sistemas de inteligência artifical.

Art. 168. Os ajustes, acordos, protocolos de intenções e outros instrumentos congêneres deverão seguir as prescrições previstas para a celebração de contratos e convênios, no que for aplicável.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 169. No tocante a ativos de informação e informação sigilosa, aplica-se,

subsidiariamente aos procedimentos previstos nestas IG, o contido na Lei nº 13.709, de 2018 , no Decreto nº 6.666, de 27 de novembro de 2008, no Decreto nº 9.637, de 26 de dezembro de 2018, na Política de Segurança da Informação para o Sistema Militar de Comando e Controle (MD31-P-03), no Conceito Operacional do Sistema de Informação e de Apoio à Decisão para Comando e Controle (MD31-S-04), na Diretriz Estratégica Organizadora do Sistema de Informação do Exército (EB10-D-01.002), na Política de Tecnologia da Informação e Comunicações do Exército (EB10-P-01.000), nas Instruções Gerais do Ciclo de Vida de **Software** (EB10-IG-01.006), nas Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro (EB10-IG-01.014), nas Instruções Gerais para a Concessão de Credencial de Segurança para o Tratamento de Informação Classificada (EB10-IG-01.017), nas Normas de Ação para a Salvaguarda das Informações Relacionadas com as Atividades de Inteligência do Sinal e de Guerra Eletrônica no Âmbito do Exército (NSISGE), nas Instruções Reguladoras sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro (IR 13-15) e nas Instruções Reguladoras sobre Segurança da Infraestrutura de Chaves Públicas do Exército Brasileiro (IR 80-05).

Art. 170. A segurança da informação sigilosa é responsabilidade do militar que tenha acesso a essas informações, estando sujeito às regras referentes ao sigilo profissional, em razão do ofício, da legislação vigente e do Estatuto dos Militares.

Art. 171. A segurança da informação sigilosa é responsabilidade do servidor civil que tenha acesso a essas informações, no âmbito do EB, estando sujeito às regras referentes ao sigilo profissional, em razão do ofício, da legislação vigente e do Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.

Art. 172. Fica resguardado o direito de indenização pelo dano material ou moral decorrente da violação do sigilo, sem prejuízo das ações penal, civil e administrativa.

Art. 173. Constituem condutas ilícitas que ensejam responsabilidade civil, administrativa e ou penal do militar ou civil as previstas no art. 32 da Lei nº 12.527, de 2011.

Art. 174. O tratamento de informação classificada resultante de tratados, acordos ou atos internacionais atenderá às normas e recomendações desses instrumentos e à legislação específica do Exército sobre o assunto.

ANEXO A

TERMO DE INVENTÁRIO DE DOCUMENTOS E/OU MATERIAIS CONTROLADOS

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22, 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
(CONTINUAÇÃO DO CABEÇALHO DA OM)

TERMO DE INVENTÁRIO DE DOCUMENTOS E/OU MATERIAIS CONTROLADOS

Nº ____/____

Inventário do(s) _____ (DOCUMENTOS E/OU MATERIAIS), controlado(s) pelo(a)_____ (ÓRGÃO CONTROLADOR)_____, nos termos do art. 63 das Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011).

Título Convencional	Nº do Exemplar / Nº de Série

_____, _____ de _____ de _____
(LOCAL E DATA)

_____
(Nome completo, Posto, Identidade e Função do Detentor)

Testemunhas:

_____
(Nome completo, Posto, Identidade e Função)

_____
(Nome completo, Posto, Identidade e Função)

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22, 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

ANEXO B

TERMO DE TRANSFERÊNCIA DE GUARDA DE DOCUMENTOS E/OU MATERIAIS CONTROLADOS

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
(CONTINUAÇÃO DO CABEÇALHO DA OM)

TERMO DE TRANSFERÊNCIA DE GUARDA DE DOCUMENTOS E/OU MATERIAIS CONTROLADOS

Nº ____/____

Ao(s) _____ dia(s) do mês de _____ do ano de dois mil e _____, em cumprimento ao disposto no art. 64 das Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), reuniram-se na(o) _____ (OM Detentora) _____ o Sr _____ (Nome Completo, Posto, Identidade e Função) _____, substituído, e o Sr _____ (Nome Completo, Posto, Identidade e Função) _____, substituto, para conferir os (documentos e/ou materiais) controlados, produzidos e recebidos pela(o) _____, então sob a custódia do primeiro, constantes do Termo de Inventário nº ____/____, anexo ao presente termo, os quais, nesta data, passam para a custódia do segundo.

Cumpridas as formalidades exigidas e conferidas todas as peças constantes do termo de inventário, foram essas julgadas (conforme ou com as seguintes alterações), sendo, para constar, lavrado o presente termo de transferência, em 3 (três) vias, datadas e assinadas pelo substituído e pelo substituto.

_____, _____ de _____ de _____
(LOCAL E DATA)

_____
(Nome completo, Posto, Identidade e Função do Substituído)

_____
(Nome completo, Posto, Identidade e Função do Substituto)

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

ANEXO C

MARCAÇÃO PARA INFORMAÇÕES, MATERIAIS E ÁREAS SIGILOSAS

a. Documentos classificados:

ULTRASSECRETO	SECRETO	RESERVADO

b. Documento preparatório – acesso restrito:

DOCUMENTO PREPARATÓRIO - ACESSO RESTRITO

Art. 3º, Inciso XII, e Art. 20 do Dec nº 7.724, de 16 de maio de 2012

c. Informação pessoal – acesso restrito:

INFORMAÇÃO PESSOAL - ACESSO RESTRITO

Art. 5º, Inciso X, da Constituição Federal do Brasil/1988
Art. 31 da Lei nº 12.527, de 18 de novembro de 2011
Art. 55 ao Art. 62 do Dec nº 7.724, de 16 de maio de 2012

d. Informação de pesquisa e desenvolvimento:

INFORMAÇÃO DE P&D - ACESSO RESTRITO

Art. 7º, §1º, da Lei nº 12.527, de 18 de novembro de 2011
Art. 6º, Inciso II, do Dec nº 7.724, de 16 de maio de 2012

e. Material de acesso restrito:

MATERIAL DE ACESSO RESTRITO

Art. 44 e 45 do Dec nº 7.845, de 14 de novembro de 2012

f. Área de acesso restrito:

(Nome da OM)

ÁREA DE ACESSO RESTRITO
Entrada proibida a pessoas não autorizadas
Art. 42 do Dec nº 7.845, de 14 de novembro de 2012

g. Cópia de documento sigiloso

CÓPIA DE DOCUMENTO SIGILOSO

O responsável deverá destruí-la quando se tornar inservível
Art. 102 das Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011)

h. Cópia extra:

Cópia Extra Nº _____

ANEXO D

TERMO DE ELIMINAÇÃO DE CÓPIA(S) DE DOCUMENTO CONTROLADO

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
(CONTINUAÇÃO DO CABEÇALHO DA OM)

TERMO DE ELIMINAÇÃO DE CÓPIA DE DOCUMENTO CONTROLADO
Nº ____/___

Ao(s) ____ dia(s) do mês de _____ do ano de dois mil e ____, em cumprimento ao disposto no art. 112 das Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), reuniram-se no(a) _____ (ORGANIZAÇÃO MILITAR) o Sr _____ (NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DA AUTORIDADE QUE CLASSIFICOU O ORIGINAL), o Sr _____ (NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DA PRIMEIRA TESTEMUNHA) e o Sr _____ (NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DA SEGUNDA TESTEMUNHA), os dois últimos como testemunhas, para proceder à eliminação da(s) cópia(s) do(s) documento(s) controlado(s) (DC) pelo(a) _____ (ÓRGÃO CONTROLADOR).

Cumpridas as formalidades exigidas e conferidas todas as peças constantes do termo de eliminação, foi(ram) eliminada(s) a(s) cópia(s) do DC abaixo discriminado(s):

Título Convencional	Nº de Exemplar

E, para constar, foi lavrado o presente Termo de Eliminação, que se acha digitado, assinado pela autoridade que classificou o original, datado e assinado pelas testemunhas, todas acima qualificadas.

AUTORIDADE QUE CLASSIFICOU O ORIGINAL:
(ou AUTORIDADE QUE MANTÉM A CUSTÓDIA):

_____, _____ de _____ de _____
(LOCAL E DATA)

_____
(Nome completo, Posto, Identidade e Função do Detentor)

Testemunhas:

_____
(Nome completo, Posto, Identidade e Função)

_____
(Nome completo, Posto, Identidade e Função)

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

ANEXO E

TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
(CONTINUAÇÃO DO CABEÇALHO DA OM)

TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO

Eu, _____ (NOME COMPLETO) _____, BRASILEIRO, CPF nº _____ (Nº, DATA E LOCAL DE EXPEDIÇÃO DO CPF) _____, FILIAÇÃO e ENDEREÇO, _____ (PRESTADOR DE SERVIÇO NA - CITAR EMPRESA) (MILITAR SERVINDO NO - CITAR OM) _____ (CITAR ÓRGÃO / OM) _____ perante o/a _____, declaro ter ciência inequívoca da legislação sobre o tratamento de informação classificada ou sob restrição de acesso cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado e me comprometo a guardar o sigilo necessário, nos termos da Lei nº 12.527, de 18 de novembro de 2011, e a:

a) tratar as informações ou materiais classificados ou sob restrição de acesso que me forem fornecidos pelo/a _____ (CITAR ÓRGÃO / OM) _____ e preservar o seu sigilo, de acordo com a legislação vigente;

b) preservar o conteúdo das informações ou materiais classificados ou sob restrição de acesso, sem divulgá-los a terceiros;

c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações ou materiais classificados ou sob restrição de acesso, ou dos materiais; e

d) não copiar ou reproduzir, por qualquer meio ou modo:

(1) informações classificadas ou sob restrição de acesso; e

(2) informações relativas aos materiais de acesso restrito do _____ (CITAR ÓRGÃO / OM) _____, salvo autorização da autoridade competente.

Declaro que _____ (RECEBI o/a) (TIVE ACESSO ao/à) _____ (DOCUMENTO OU MATERIAL ENTREGUE OU EXIBIDO AO SIGNATÁRIO) _____ e, por estar de acordo com o presente Termo, assino na presença das testemunhas abaixo identificadas.

Declaro, ainda, que consinto e concordo que o/a _____ (CITAR ÓRGÃO / OM) _____ realize o tratamento de meus dados pessoais, envolvendo operações como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, com a finalidade de _____ (CITAR A FINALIDADE DA REALIZAÇÃO DO TRATAMENTO DO DADO PESSOAL) _____, nos termos do inciso I do art. 7º da Lei nº 13.709, de 14 de agosto de 2018, lei geral de proteção de dados pessoais.

_____, _____ de _____ de _____

(LOCAL E DATA)

_____

(Nome completo, Posto, Identidade e Função)

Testemunhas:

_____

(Nome completo, Posto, Identidade e Função)

_____

(Nome completo, Posto, Identidade e Função)

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

ANEXO F

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO

ULTRASSECRETO

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO	
ÓRGÃO/ENTIDADE: (OM que produziu)	
CÓDIGO DE INDEXAÇÃO: (1)	
GRAU DE SIGILO: **ULTRASSECRETO**	
CATEGORIA: **05** (2)	
TIPO DE DOCUMENTO: (Ofício, DIEx etc.)	
DATA DE PRODUÇÃO: (data da assinatura do documento)	
FUNDAMENTO LEGAL PARA A CLASSIFICAÇÃO: inciso (I a VIII) do art. 23 da Lei nº 12.527, de 18 de novembro de 2011.	
RAZÕES PARA A CLASSIFICAÇÃO: – **ULTRASSECRETO** (3)	
ASSUNTO DA INFORMAÇÃO CLASSIFICADA (**Conforme o previsto no inciso VII do art. 31 do Dec nº 11.527, de 16 de maio de 2023)**	
PRAZO DA RESTRIÇÃO DE ACESSO: (4)	
DATA DE CLASSIFICAÇÃO: (DD/MM/AAAA da assinatura deste TCI)	
AUTORIDADE CLASSIFICADORA	Nome: Cargo:
AUTORIDADE RATIFICADORA	Nome: Cargo:
DESCLASSIFICAÇÃO em DD/MM/AAAA	Nome: Cargo:
RECLASSIFICAÇÃO em DD/MM/AAAA	Nome: Cargo:
REDUÇÃO DE PRAZO em DD/MM/AAAA	Nome: Cargo:
PRORROGAÇÃO DE PRAZO em DD/MM/AAAA	Nome: Cargo:
_____ ASSINATURA DA AUTORIDADE CLASSIFICADORA	
_____ ASSINATURA DA AUTORIDADE RATIFICADORA	
_____ ASSINATURA DA AUTORIDADE RESPONSÁVEL POR DESCLASSIFICAÇÃO	
_____ ASSINATURA DA AUTORIDADE RESPONSÁVEL POR RECLASSIFICAÇÃO	
_____ ASSINATURA DA AUTORIDADE RESPONSÁVEL POR REDUÇÃO DE PRAZO	
_____ ASSINATURA DA AUTORIDADE RESPONSÁVEL POR PRORROGAÇÃO DE PRAZO	

ULTRASSECRETO

SECRETO

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO	
ÓRGÃO/ENTIDADE: (OM que produziu)	
CÓDIGO DE INDEXAÇÃO: (1)	
GRAU DE SIGILO: **SECRETO**	
CATEGORIA: **05** (2)	
TIPO DE DOCUMENTO: (Ofício, DIEx etc.)	
DATA DE PRODUÇÃO: (data da assinatura do documento)	
FUNDAMENTO LEGAL PARA A CLASSIFICAÇÃO: inciso (I a VIII) do art. 23 da Lei nº 12.527, de 18 de novembro de 2011.	
RAZÕES PARA A CLASSIFICAÇÃO: - **SECRETO** (3)	
ASSUNTO DA INFORMAÇÃO CLASSIFICADA (**Conforme o previsto no inciso VII do art. 31 do Dec nº 11.527, de 16 de maio de 2023)**	
PRAZO DA RESTRIÇÃO DE ACESSO: (4)	
DATA DE CLASSIFICAÇÃO: (DD/MM/AAAA da assinatura deste TCI)	
AUTORIDADE CLASSIFICADORA	Nome: Cargo:
DESCLASSIFICAÇÃO em DD/MM/AAAA	Nome: Cargo:
RECLASSIFICAÇÃO em DD/MM/AAAA	Nome: Cargo:
REDUÇÃO DE PRAZO em DD/MM/AAAA	Nome: Cargo:
_____ ASSINATURA DA AUTORIDADE CLASSIFICADORA	
_____ ASSINATURA DA AUTORIDADE RESPONSÁVEL POR DESCLASSIFICAÇÃO	
_____ ASSINATURA DA AUTORIDADE RESPONSÁVEL POR RECLASSIFICAÇÃO	
_____ ASSINATURA DA AUTORIDADE RESPONSÁVEL POR REDUÇÃO DE PRAZO	

SECRETO

RESERVADO

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO	
ÓRGÃO/ENTIDADE: (OM que produziu)	
CÓDIGO DE INDEXAÇÃO: (1)	
GRAU DE SIGILO: **RESERVADO**	
CATEGORIA: **05** (2)	
TIPO DE DOCUMENTO: (Ofício, DIEx etc.)	
DATA DE PRODUÇÃO: (data da assinatura do documento)	
FUNDAMENTO LEGAL PARA A CLASSIFICAÇÃO: inciso (I a VIII) do art. 23 da Lei nº 12.527, de 18 de novembro de 2011.	
ASSUNTO DA INFORMAÇÃO CLASSIFICADA (**Alinhamento com o previsto no inciso VII do art. 31 do Dec nº 11.527, de 16 de maio de 2023)**	
RAZÕES PARA A CLASSIFICAÇÃO: – **RESERVADO** (3)	
PRAZO DA RESTRIÇÃO DE ACESSO: (4)	
DATA DE CLASSIFICAÇÃO: (DD/MM/AAAA da assinatura deste TCI)	
AUTORIDADE CLASSIFICADORA	Nome: Cargo:
DESCLASSIFICAÇÃO em DD/MM/AAAA	Nome: Cargo:
REDUÇÃO DE PRAZO em DD/MM/AAAA	Nome: Cargo:
_____ ASSINATURA DA AUTORIDADE CLASSIFICADORA	
_____ ASSINATURA DA AUTORIDADE RESPONSÁVEL POR DESCLASSIFICAÇÃO	
_____ ASSINATURA DA AUTORIDADE RESPONSÁVEL POR REDUÇÃO DE PRAZO	

Legenda:

(1) Código de Indexação de Documento que Contém Informação Classificada.
Exemplo: **11111.000001/2013-99.U.05.05/12/2012.05/12/2037.N**

NUP/NUD	Grau de sigilo	Categoria	Data de Produção	Data de Desclassificação	Indicação da Reclassificação	Data da Prorrogação (U)
	U, S ou R	01 a 17	DD/MM/AAAA	DD/MM/AAAA	S ou N	DD/MM/AAAA
11111.000001/2013-99	U	05	05/12/2012	05/12/2037	N	

(2) No campo "CATEGORIA", deve ser registrado o número "05", que equivale à categoria "Defesa e Segurança".

(3) O campo "RAZÕES PARA A CLASSIFICAÇÃO" é destinado à análise pela Comissão Mista de Reavaliação de Informações. A redação não poderá ser cópia do inciso do fundamento legal. Deve-se procurar explicar o motivo pelo qual o documento em questão deve ser classificado.

Ex: Para TCI de documento SECRETO

RAZÕES PARA A CLASSIFICAÇÃO: – SECRETO Sua divulgação pode causar embaraço diplomático com país vizinho.

(4) No campo "PRAZO DA RESTRIÇÃO DE ACESSO", deve ser fixado o tempo em anos, no prazo máximo para cada classificação. Ex: até 5 anos (ERRADO); 5 anos (CERTO).

ANEXO G

IDENTIFICAÇÃO DE CÓPIA DE DOCUMENTO SIGILOSO

CLASSIFICAÇÃO SIGILOSA

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
(CONTINUAÇÃO DO CABEÇALHO DA OM)

DIEx nº _____

EB: _____

_____ – ___, de _____ de ____

Do:

Ao:

Assunto:

Referência:

Anexo:

1. _____

_____

_____

_____

_____

_____

2. _____

_____

_____

_____, _____ de _____ de _____
(LOCAL E DATA)

_____
(Nome completo, Posto e Função)

CLASSIFICAÇÃO SIGILOSA

A140872

ANEXO H

TERMO DE ELIMINAÇÃO DE MATERIAL CONTROLADO

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
(CONTINUAÇÃO DO CABEÇALHO DA OM)

TERMO DE ELIMINAÇÃO DE MATERIAL CONTROLADO

Nº ____/___

Ao(s) ____ dia(s) do mês de _____ do ano de dois mil e ____, em cumprimento ao inciso II do art. 125 das Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), reuniram-se no(a) _____ (NOME DA OM) _____ o Sr _____ (NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DA AUTORIDADE QUE CLASSIFICOU O ORIGINAL) _____, o Sr _____ (NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DE UMA DAS TESTEMUNHAS) _____ e o Sr _____ (NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DA OUTRA TESTEMUNHA) _____, os dois últimos como testemunhas, para proceder à eliminação do(s) material(is) controlado(s) (MC), pelo(a) _____ (ÓRGÃO CONTROLADOR) _____.

Cumpridas as formalidades exigidas e conferidas todas as peças constantes do termo de eliminação, foi(ram) eliminado(s) o(s) MC abaixo discriminado(s):

Título Convencional	Nº de Série

E, para constar, foi lavrado o presente Termo de Eliminação.

Detentor:

_____, _____ de _____ de _____
(LOCAL E DATA)

_____
(Nome completo, Posto e Função)

Testemunhas:

_____
(Nome completo, Posto, Identidade e Função)

_____
(Nome completo, Posto, Identidade e Função)

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

ANEXO I

RESUMO EXPLICATIVO PARA PROPOSTA DE TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

MINISTÉRIO DA DEFESA **EXÉRCITO BRASILEIRO** (CONTINUAÇÃO DO CABEÇALHO DA OM)	_____ (OM) Visto do(a) Cmt/Ch/Dir do _____

Resumo explicativo do documento de NUP/NUD nº _____

Texto.

_____

_____

_____

_____

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

ANEXO J

TERMO DE CUSTÓDIA DE MATERIAL/DOCUMENTO CONTROLADO

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
(CONTINUAÇÃO DO CABEÇALHO DA OM)

TERMO DE CUSTÓDIA DE MATERIAL/DOCUMENTO CONTROLADO

Nº ____/___

Ao(s) _____ dia(s) do mês de _____ do ano de dois mil e _____, o Sr_____(Nome Completo, Posto, Identidade e Função da Autoridade que assume a Custódia Do DC/MC)_____, assume a custódia do(s) exemplar(es) nº _____(Nº do DC/MC)_____ do _____(Título Convencional do DC/MC)_____, datado de _____(Data do DC/MC)_____.

Cumpridas as formalidades exigidas e conferidas todas as peças constantes do _____(Título Convencional do DC/MC)_____, foram julgados _____(Conforme ou com as seguintes alterações)_____, sendo, para constar, lavrado o presente Termo de Custódia, em 2 (duas) vias, assinado e datado pelo responsável pela sua guarda.

Detentor:

_____, _____ de _____ de _____

(LOCAL E DATA)

_____

(Nome completo, Posto, Função e Identidade)

DOCUMENTO DE ACESSO RESTRITO

Art. 21, 22 e 42 ao 47 do Dec nº 7.845, de 14 de novembro de 2012